

# Sun Ethernet Fabric Operating System CLI Reference Manual, Vol. 6

**ORACLE**

Part No: E60930-02

August 2015

Copyright © 2015, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

#### Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

#### Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Copyright © 2015, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf stipulation expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée d'The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

#### Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

#### Accès au support électronique

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le [site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info](http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info) ou le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> si vous êtes malentendant.

# Contents

---

<b>Using This Documentation.....</b>	<b>11</b>
<b>34. IGMP Snooping .....</b>	<b>13</b>
34.1 ip igmp snooping.....	14
34.2 ip igmp snooping proxy-reporting .....	16
34.3 snooping multicast-forwarding-mode.....	17
34.4 ip igmp snooping mrouter-time-out.....	18
34.5 ip igmp querier-timeout .....	19
34.6 ip igmp snooping port-purge-interval .....	20
34.7 ip igmp snooping source-only learning age-timer.....	21
34.8 ip igmp snooping report-suppression interval.....	22
34.9 ip igmp snooping retry-count .....	23
34.10 ip igmp snooping group-query-interval .....	24
34.11 ip igmp snooping report-forward.....	25
34.12 ip igmp snooping query-forward .....	26
34.13 ip igmp snooping version .....	27
34.14 ip igmp snooping fast-leave .....	28
34.15 ip igmp snooping vlan - immediate leave .....	29
34.16 ip igmp snooping querier .....	30
34.17 ip igmp snooping query-interval.....	31
34.18 ip igmp snooping startup-query-interval .....	32
34.19 ip igmp snooping startup-query-count .....	33
34.20 ip igmp snooping other-querier-present-interval.....	34
34.21 ip igmp snooping mrouter .....	35
34.22 ip igmp snooping vlan mrouter.....	37
34.23 shutdown snooping.....	39
34.24 debug ip igmp snooping.....	40
34.25 snooping leave-process config-level .....	42
34.26 snooping report-process config-level.....	43
34.27 mvr .....	44
34.28 ip igmp snooping blocked-router.....	45
34.29 ip igmp snooping multicast-vlan profile.....	47
34.30 ip igmp snooping leavemode .....	48
34.31 ip igmp snooping ratelimit .....	50

34.32 ip igmp snooping limit .....	52
34.33 ip igmp snooping filter-profileid .....	54
34.34 ip igmp snooping proxy .....	56
34.35 ip igmp snooping max-response-code .....	57
34.36 ip igmp snooping mrouter-port -time-out .....	58
34.37 ip igmp snooping mrouter-port-version .....	60
34.38 show ip igmp snooping mrouter .....	62
34.39 show ip igmp snooping mrouter - Redundancy .....	64
34.40 show ip igmp snooping globals .....	66
34.41 show ip igmp snooping .....	69
34.42 show ip igmp snooping - Redundancy .....	71
34.43 show ip igmp snooping groups .....	73
34.44 show ip igmp snooping forwarding-database .....	77
34.45 show ip igmp snooping forwarding-database - Redundancy .....	79
34.46 show ip igmp snooping statistics .....	81
34.47 show ip igmp snooping blocked-router .....	85
34.48 show ip igmp snooping multicast-receivers .....	87
34.49 show ip igmp snooping port-cfg .....	89
34.50 show ip igmp snooping multicast-vlan .....	93
34.51 ip igmp snooping clear counters .....	95
34.52 ip igmp snooping send-query .....	96
34.53 ip igmp snooping static-group .....	97
34.54 ip igmp filter .....	99
34.55 ip igmp max-groups .....	100
<b>35. MLD Snooping .....</b>	<b>101</b>
35.1 ipv6 mld snooping .....	102
35.2 ipv6 mld snooping proxy-reporting .....	103
35.3 ipv6 mld snooping mrouter-time-out .....	104
35.4 ipv6 mld snooping port-purge-interval .....	105
35.5 ipv6 mld snooping report-suppression-interval .....	106
35.6 ipv6 mld snooping retry-count .....	107
35.7 ipv6 mld snooping group-query-interval .....	108
35.8 ipv6 mld snooping report-forward .....	109
35.9 ipv6 mld snooping version .....	110
35.10 ipv6 mld snooping fast-leave .....	111
35.11 ipv6 mld snooping querier .....	112
35.12 ipv6 mld snooping query-interval .....	113

35.13	ipv6 mld snooping mrouter .....	114
35.14	debug ipv6 mld snooping .....	116
35.15	show ipv6 mld snooping mrouter .....	118
35.16	show ipv6 mld snooping globals .....	120
35.17	show ipv6 mld snooping .....	123
35.18	show ipv6 mld snooping groups .....	126
35.19	show ipv6 mld snooping forwarding-database .....	128
35.20	show ipv6 mld snooping statistics .....	130
35.21	ipv6 mld snooping clear counters .....	133
35.22	debug ipv6 mld snooping all .....	134
<b>36.</b>	<b>IGMP .....</b>	<b>135</b>
36.1	set ip igmp .....	136
36.2	ip igmp immediate-leave .....	137
36.3	ip igmp version .....	138
36.4	ip igmp query-interval .....	139
36.5	ip igmp query-max-response-time .....	140
36.6	ip igmp robustness .....	141
36.7	ip igmp last-member-query-interval .....	142
36.8	ip igmp static-group .....	143
36.9	no ip igmp .....	144
36.10	debug ip igmp .....	145
36.11	show ip igmp global-config .....	146
36.12	show ip igmp interface .....	147
36.13	show ip igmp groups .....	150
36.14	show ip igmp sources .....	151
36.15	show ip igmp statistics .....	152
36.16	show provider-bridge tunnel-mac-address .....	155
36.17	ip igmp limit .....	156
36.18	ip igmp group-list .....	157
36.19	ip igmp limit - except group list id .....	158
36.20	show ip igmp group-list .....	159
36.21	ip igmp explicit-tracking .....	160
36.22	show ip igmp membership .....	161
<b>37.</b>	<b>IGMP Proxy .....</b>	<b>163</b>
37.1	ip igmp proxy-service .....	164
37.2	ip igmp proxy service .....	165

37.3	ip igmp-proxy mrouter .....	166
37.4	ip igmp mroute proxy .....	167
37.5	ip igmp-proxy mrouter-time-out.....	168
37.6	ip igmp-proxy mrouter-version .....	169
37.7	show ip igmp-proxy mrouter .....	170
37.8	show ip igmp-proxy forwarding-database.....	172
<b>38.</b>	<b>PIM.....</b>	<b>175</b>
38.1	set ip pim.....	176
38.2	ip multicast.....	179
38.3	ip pim version.....	182
38.4	set ip pim threshold.....	183
38.5	set ip pim spt-switchperiod .....	184
38.6	set ip pim rp-threshold .....	185
38.7	set ip pim rp-switchperiod .....	186
38.8	set ip pim regstop-ratelimit-period .....	187
38.9	set ip pim pmbr .....	188
38.10	ip pim component .....	189
38.11	set ip pim static-rp.....	191
38.12	set ip pim state-refresh origination-interval.....	192
38.13	ip pim state-refresh disable.....	193
38.14	set ip pim source-active interval .....	194
38.15	set mode .....	195
38.16	rp-candidate rp-address.....	196
38.17	rp-candidate holdtime .....	198
38.18	rp-static rp-address .....	199
38.19	ip pim query-interval .....	201
38.20	ip pim message-interval.....	202
38.21	ip pim bsr-candidate - value.....	203
38.22	ip pim bsr-candidate – vlan.....	205
38.23	ip pim componentId .....	207
38.24	ip pim dr-priority .....	209
38.25	ip pim override-interval .....	210
38.26	ip pim lan-delay.....	211
38.27	set ip pim lan-prune-delay .....	212
38.28	set ip pim graft-retry interval .....	213
38.29	no ip pim interface .....	214
38.30	debug ip pim .....	215

38.31	show ip pim interface .....	217
38.32	show ip pim neighbor .....	221
38.33	show ip pim rp-candidate .....	223
38.34	show ip pim rp-set.....	225
38.35	show ip pim bsr .....	227
38.36	show ip pim rp-static .....	228
38.37	show ip pim component .....	230
38.38	show ip pim thresholds .....	231
38.39	show ip pim mroute.....	233
38.40	show ip pim redundancy state .....	235
38.41	show ip pim redundancy shadow-table .....	236
38.42	ip pim bsr-border.....	237
38.43	set ip pim rpf vector .....	238
38.44	ip pim bidir-enable .....	239
38.45	ip pim bidir-offer-interval .....	241
38.46	ip pim bidir-offer-limit .....	242
38.47	show ip pim rp-hash.....	243
38.48	ip pim external border .....	244
38.49	show ip pim interface df .....	245
<b>39.</b>	<b>PIMv6.....</b>	<b>247</b>
39.1	set ipv6 pim.....	248
39.2	set ip pim threshold.....	251
39.3	set ip pim spt-switchperiod .....	252
39.4	set ip pim rp-threshold .....	253
39.5	set ip pim rp-switchperiod .....	254
39.6	set ip pim regstop-ratelimit-period .....	255
39.7	set ip pim pmbr .....	256
39.8	set ip pim static-rp.....	257
39.9	ip pim component .....	258
39.10	ipv6 pim rp-candidate rp-address .....	260
39.11	ipv6 pim rp-static rp-address .....	262
39.12	ipv6 pim query-interval.....	264
39.13	ipv6 pim message-interval .....	265
39.14	ipv6 pim bsr-candidate.....	266
39.15	ipv6 pim componentId.....	267
39.16	ipv6 pim hello-holdtime .....	269
39.17	ipv6 pim dr-priority .....	270

39.18	ipv6 pim override-interval.....	271
39.19	ipv6 pim lan-delay.....	272
39.20	set ipv6 pim lan-prune-delay.....	273
39.21	set ipv6 pim graft-retry interval.....	274
39.22	no ipv6 pim interface.....	275
39.23	debug ipv6 pim.....	276
39.24	show ipv6 pim interface.....	278
39.25	show ipv6 pim neighbor.....	281
39.26	show ipv6 pim rp-candidate.....	283
39.27	show ipv6 pim rp-set.....	284
39.28	show ipv6 pim bsr.....	286
39.29	show ipv6 pim rp-static.....	287
39.30	show ipv6 pim component.....	289
39.31	show ipv6 pim thresholds.....	290
39.32	show ipv6 pim mroute.....	292
39.33	show ip pim redundancy state.....	294
39.34	show ipv6 pim redundancy shadow-table.....	295
39.35	ipv6 pim bsr-border.....	296
39.36	embedded-rp.....	297
39.37	ip pim bidir-enable.....	299
39.38	ip pim bidir-offer-interval.....	301
39.39	ip pim bidir-offer-limit.....	302
39.40	show ipv6 pim rp-hash.....	303
<b>40.</b>	<b>IPv4 Multicasting.....</b>	<b>305</b>
40.1	ip multicast routing.....	306
40.2	ip multicast-routing.....	307
40.3	ip mcast ttl-threshold.....	308
40.4	ip mcast rate-limit.....	310
40.5	show ip mroute.....	311
<b>41.</b>	<b>TAC.....</b>	<b>313</b>
41.1	ip mcast profile.....	314
41.2	ip igmp profile.....	316
41.3	set ip mcast profiling.....	317
41.4	permit.....	318
41.5	deny.....	319
41.6	range.....	320



41.7	profile active.....	321
41.8	show ip mcast profile .....	322
41.9	debug tacm .....	324
<b>42.</b>	<b>RMON.....</b>	<b>325</b>
42.1	set rmon.....	326
42.2	rmon collection history .....	327
42.3	rmon collection stats .....	329
42.4	rmon event .....	330
42.5	rmon alarm.....	331
42.6	show rmon .....	333
<b>43.</b>	<b>RMON2.....</b>	<b>337</b>
43.1	rmon2.....	338
43.2	debug rmon2.....	339



# Using This Documentation

---

- **Overview** – Provides information on Oracle's SEFOS CLI commands
- **Audience** – Users and system administrators who configure SEFOS through the CLI
- **Required knowledge** – Basic knowledge of UNIX CLI command syntax

## Product Documentation Library

Documentation and resources for this product and related products are available at [http://www.oracle.com/goto/es2-72\\_es2-64/docs](http://www.oracle.com/goto/es2-72_es2-64/docs).

## Acronyms

Refer to the *Sun Ethernet Fabric Operating System CLI Reference Manual, Vol. 1* for acronyms and abbreviations.

## CLI Command Modes

Refer to the *Sun Ethernet Fabric Operating System CLI Reference Manual, Vol. 1* for CLI command modes.

## Feedback

Provide feedback about this documentation at <http://www.oracle.com/goto/docfeedback>.



# IGMP Snooping

---

Internet Group Multicast Protocol, (IGMP) is the protocol a host uses to inform a router when it joins (or leaves) an Internet multicast group. IGMP is only used on a local network. A router must use another multicast routing protocol to inform other routers of group membership. IGMP Snooping (IGS) is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers. In IGS, a host computer uses IGMP to inform a router that it intends to listen to a specific multicast address. If another computer snoops such packets, it can learn the multicast sessions to which other computers on the local network are listening. The multicast packet transfer happens only between the source and the destination computers. Broadcasting of packets is avoided. IGMP snooping significantly reduces traffic from streaming media and other bandwidth-intensive IP multicast applications.

The list of CLI commands for the configuration of IGS is common to both single instance and multiple instance except for a difference in the prompt that appears for the switch with multiple instance support.

The prompt for the Global Configuration mode is,

```
SEFOS(config)#
```

## 34.1 ip igmp snooping

---

**Command Objective** This command enables IGMP snooping in the switch or a specific VLAN. When snooping is enabled in a switch or interface, it learns the host's intention to listen to a specific multicast address. When the switch receives any packet from the specified multicast address, it forwards the packet to the host listening for that address. Broadcasting is avoided to save bandwidth. When IGMP snooping is enabled globally, it is enabled in all the existing VLAN interfaces.

The no form of the command disables IGMP snooping in the switch or a specific VLAN. When IGMP snooping is disabled globally, it is disabled in all the existing VLAN interfaces.

---

### Syntax

#### Global Configuration Mode

```
ip igmp snooping [vlan <vlanid/vfi_id>]
```

```
no ip igmp snooping [vlan <vlanid/vfi_id>]
```

#### Config-VLAN Mode

```
ip igmp snooping
```

```
no ip igmp snooping
```

---

### Parameter Description

- **vlan <vlan-id/vfi-id>** - Enables IGMP snooping for the specified VLAN / VFI ID. This value ranges from 1 to 65535.
  - **<vlan -id>** - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.
  - **<vfi-id>** - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.

---

Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.

Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.

Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.

---

<b>Mode</b>	Global Configuration Mode / Config-VLAN Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	IGMP snooping is disabled globally and in all VLANs.
<u>Note:</u>	GMRP has to be disabled to enable IGMP snooping.
<b>Example</b>	<pre>SEFOS(config)# ip igmp snooping SEFOS(config-vlan)# ip igmp snooping</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"> <li>• <b>shutdown snooping</b> - Shuts down IGMP snooping in the switch.</li> <li>• <b>ip igmp snooping fast-leave / ip igmp snooping vlan - immediate leave</b> - Enables fast leave processing and IGMP snooping for a specific VLAN.</li> <li>• <b>show ip igmp snooping</b> - Displays IGMP snooping information for all VLANs or a specific VLAN.</li> <li>• <b>show ip igmp snooping globals</b> - Displays the IGMP snooping information for all VLANs or a specific VLAN.</li> <li>• <b>snooping multicast-forwarding-mode</b> – Specifies the snooping multicast forwarding mode.</li> <li>• <b>show ip igmp snooping multicast-receivers</b> – Displays IGMP multicast host information for all VLANs, a specific VLAN, or specific VLAN and group address, for a given switch or for all switches (if no switch is specified).</li> <li>• <b>show ip igmp forwarding-database</b> - Displays multicast forwarding entries.</li> </ul>

## 34.2 ip igmp snooping proxy-reporting

---

<b>Command Objective</b>	<p>This command enables proxy-reporting in the IGMP snooping switch. When enabled, the switch supports the multicast router in learning the membership information of the multicast group. It forwards the multicast packets based on group membership information. The proxy-reporting switch acts as a querier to the downstream hosts. It sends proxy-reporting to upstream queriers.</p> <p>The no form of the command disables proxy-reporting in the IGMP snooping switch.</p>
<b>Syntax</b>	<pre>ip igmp snooping proxy-reporting</pre> <pre>no ip igmp snooping proxy-reporting</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	Proxy-reporting is enabled.
	<p><u>Note:</u> Proxy-reporting can be enabled in the IGMP snooping switch only if the proxy is disabled in the switch.</p>
<b>Example</b>	<pre>SEFOS(config)# ip igmp snooping proxy-reporting</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>no ip igmp snooping proxy</code> – Disables proxy in the IGMP snooping switch.</li><li>• <code>show ip igmp snooping globals</code> - Displays the IGMP snooping information for all VLANs or a specific VLAN.</li><li>• <code>show ip igmp forwarding-database</code> - Displays multicast forwarding entries.</li></ul>

---



## 34.3 snooping multicast-forwarding-mode

---

<b>Command Objective</b>	This command specifies the snooping multicast forwarding mode (IP-based or MAC-based). When <code>ip</code> mode is selected, and PIM and IGS are enabled, the L3 bitmap in the IPMC table is updated by PIM. The corresponding L2 bitmap is updated by querying the IGS to obtain Portlist. When PIM is disabled, IGS updates the L2 bitmap in the IPMC table directly. When the mode is MAC-based, the L2 bitmap is updated by PIM which queries the VLAN to obtain Portlist. When PIM is disabled, the IGS updates the L2 bitmap directly.
<b>Syntax</b>	<code>snooping multicast-forwarding-mode {ip   mac}</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>ip</code> - Configures the multicast forwarding mode as IP address-based. The PIM queries the IGS module to obtain the Portlist.</li><li>• <code>mac</code> - Configures the multicast forwarding mode as MAC address-based. The PIM queries the VLAN to obtain the Portlist.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	<code>mac</code>
<b>Example</b>	<code>SEFOS(config)# snooping multicast-forwarding-mode mac</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp snooping globals</code> - Displays the IGMP snooping information for all VLANs or a specific VLAN.</li><li>• <code>ip igmp snooping enhanced-mode</code> - Enables or disables snooping system enhanced mode in the switch.</li><li>• <code>ip igmp snooping static-group</code> - Configures IGMP snooping static multicast for VLAN(s).</li></ul>

---

## 34.4 ip igmp snooping mrouter-time-out

---

<b>Command Objective</b>	<p>This command sets the IGMP snooping router port purge time-out interval. Snooping learns the available router ports and initiates router port purge time-out timer for each learned router port. The router sends control messages to the ports. If the router ports receive such control messages, the timer is restarted. If no message is received by the router ports before the timer expires, the router port entry is purged. The purge time-out value ranges between 60 and 600 seconds.</p> <p>The no form of the command sets the IGMP snooping router port purge time-out to default value.</p>
<b>Syntax</b>	<pre>ip igmp snooping mrouter-time-out &lt;(60 - 600) seconds&gt;  no ip igmp snooping mrouter-time-out</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	125 seconds
<b>Example</b>	<pre>SEFOS(config)#ip igmp snooping mrouter-time-out 70</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp snooping mrouter</code> - Displays detailed information about the router ports for all VLANs or specific VLAN.</li><li>• <code>show ip igmp snooping globals</code> - Displays the global information of IGMP snooping.</li></ul>

---

## 34.5 ip igmp querier-timeout

---

<b>Command Objective</b>	<p>This command sets the IGMP snooping router port purge time-out interval. Snooping learns the available router ports and initiates router port purge time-out timer for each learned router port. The routers send control messages to the ports. If the router ports receive such control messages, the timer is restarted. If no message is received by the router ports before the timer expires, the router port entry is purged. The purge time-out value ranges between 60 and 600 seconds.</p> <p>This command is a standardized implementation of the existing command <code>ip igmp snooping mrouter-time-out</code>. Its operation is similar to the existing command.</p>
<b>Syntax</b>	<code>ip igmp querier-timeout &lt;(60 - 600) seconds&gt;</code>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	125 seconds
<b>Example</b>	<code>SEFOS(config)#ip igmp querier-timeout 70</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp snooping mrouter</code> - Displays detailed information about the router ports for all VLANs or specific VLAN.</li><li>• <code>show ip igmp snooping globals</code> - Displays the global information of IGMP snooping.</li></ul>

---

## 34.6 ip igmp snooping port-purge-interval

---

<b>Command Objective</b>	<p>This command configures the IGMP snooping port purge time interval. When the port receives reports from hosts, the timer is initiated. If the port receives another report before the timer expires, the timer is restarted. If the port does not receive any report from hosts till the timer expires, then the port entry is purged from the multicast database. The purge time interval value ranges between 130 and 1225 seconds.</p> <p>The no form of the command sets the IGMP snooping port purge time to default value.</p>
<b>Syntax</b>	<pre>ip igmp snooping port-purge-interval &lt;(130 - 1225) seconds&gt;  no ip igmp snooping port-purge-interval</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	260 seconds
<b>Example</b>	<pre>SEFOS (config)# ip igmp snooping port-purge-interval 150</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp snooping</code> - Displays IGMP snooping information for all VLANs or a specific VLAN.</li><li>• <code>show ip igmp snooping globals</code> - Displays the IGMP snooping information for all VLANs or a specific VLAN.</li></ul>

---

## 34.7 ip igmp snooping source-only learning age-timer

---

<b>Command Objective</b>	<p>This command configures the IGMP snooping port purge time interval. When the port receives reports from hosts, the timer is initiated. If the port receives another report before the timer expires, the timer is restarted. If the port does not receive any report from hosts till the timer expires, then the port entry is purged from the multicast database. The purge time interval value ranges between 130 and 1225 seconds.</p> <p>The no form of the command resets the IGMP snooping port purge time interval to its default value.</p> <p>This command is a standardized implementation of the existing command <code>ip igmp snooping port-purge-interval</code>. Its operation is similar to the existing command.</p>
<b>Syntax</b>	<pre>ip igmp snooping source-only learning age-timer &lt;short (130-1225)&gt;  no ip igmp snooping source-only learning age-timer</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	260 seconds
<b>Example</b>	<pre>SEFOS (config)# ip igmp snooping source-only learning age- timer 200</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp snooping</code> - Displays IGMP snooping information for all VLANs or a specific VLAN.</li><li>• <code>show ip igmp snooping globals</code> - Displays the IGMP snooping information for all VLANs or a specific VLAN.</li></ul>

---

## 34.8 ip igmp snooping report-suppression interval

---

<b>Command Objective</b>	<p>This command sets the IGMP snooping report-suppression time interval. The switch forwards IGMPv2 report message to the multicast group. A timer is started immediately after forwarding the report message and runs for set period of time. During this interval the switch does not forward another IGMPv2 report message, addressed to the same multicast group, to the router ports.</p> <p>The no form of the command sets the IGMP snooping report-suppression interval time to the default value.</p>
<b>Syntax</b>	<pre>ip igmp snooping report-suppression-interval &lt;(1 - 25) seconds&gt;  no ip igmp snooping report-suppression-interval</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	5 seconds
	<p><u>Note:</u> The <code>ip igmp snooping report-suppression-interval</code> is used only when the proxy and proxy-reporting are disabled.</p>
<b>Example</b>	<pre>SEFOS(config)# ip igmp snooping report-suppression- interval 20</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp snooping globals</code> - Displays the IGMP snooping information for all VLANs or a specific VLAN.</li></ul>

---

## 34.9 ip igmp snooping retry-count

---

<b>Command Objective</b>	<p>This command sets the maximum number of group-specific queries sent by the switch to check if there are any interested v2 receivers for the group when it receives a leave message in the proxy or proxy-reporting mode. The port is deleted from the group membership information in the forwarding database if the maximum retry count exceeds set number. This value ranges from 1 to 5.</p> <p>The no form of the command sets the number of group-specific queries sent by the switch on reception of leave message to default value.</p>
<b>Syntax</b>	<pre>ip igmp snooping retry-count &lt;1 - 5&gt;  no ip igmp snooping retry-count</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	2
<b>Example</b>	<pre>SEFOS (config)# ip igmp snooping retry-count 4</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp snooping globals</code> - Displays the IGMP snooping information for all VLANs or a specific VLAN.</li><li>• <code>ip igmp snooping clear counters</code> - Clears the IGMP snooping statistics maintained for VLAN(s).</li></ul>

---

## 34.10 ip igmp snooping group-query-interval

---

**Command Objective** This command sets the time interval after which the switch sends a group-specific query to find out if there are any interested receivers in the group when it receives a leave message. If it does not receive a response from the group, the port is removed from the group membership information in the forwarding database. This value ranges from 2 to 5.

The no form of the command sets the group-specific query interval time to default value.

---

**Syntax** `ip igmp snooping group-query-interval <2-5> seconds`  
`no ip igmp snooping group-query-interval`

---

**Mode** Global Configuration Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Default** 2 seconds

---

**Example** `SEFOS(config)# ip igmp snooping group-query-interval 3`

---

**Related Command(s)**

- `show ip igmp snooping globals` - Displays the IGMP snooping information for all VLANs or a specific VLAN.
- `show ip igmp snooping statistics` - Displays IGMP snooping statistics for all VLANs or a specific VLAN.
- `show ip igmp snooping groups` - Displays IGMP group information for all VLANs or a specific VLAN.

---



## 34.11 ip igmp snooping report-forward

---

<b>Command Objective</b>	<p>This command configures the IGMP reports to be forwarded to all ports, router ports of a VLAN, or non-edge ports. The configuration enables the switch to forward IGMP report messages to the selected ports thus avoiding flooding of the network.</p> <p>The no form of the command sets IGMP report-forwarding status to default value.</p>
<b>Syntax</b>	<pre>ip igmp snooping report-forward {all-ports   router-ports   non-edge-ports }  no ip igmp snooping report-forward</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>all-ports</b> - Configures the IGMP reports to be forwarded to all the ports of a VLAN.</li><li>• <b>router-ports</b> - Configures the IGMP reports to be forwarded only to router ports of a VLAN.</li><li>• <b>non-edge-ports</b> - Configures the IGMP reports to be forwarded only to STP non edge ports.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	router-ports
	<p><u>Note:</u> In snooping mode, snooping module will forward reports only on router ports by default.</p>
<b>Example</b>	<pre>SEFOS(config)# ip igmp snooping report-forward all-ports</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>show ip igmp snooping globals</b> - Displays the IGMP snooping information for all VLANs or a specific VLAN.</li></ul>

---

## 34.12 ip igmp snooping query-forward

---

<b>Command Objective</b>	This command configures the IGMP queries to be forwarded to all VLAN member ports or only to non-router ports. This configuration directs the queries to the selected ports to avoid flooding of the network. The queries are forwarded to multicast groups. If the VLAN module is enabled, IGMP snooping sends and receives the multicast packets through VLAN module. When VLAN is disabled, it sends the multicast packets through Bridge initialization/shutdown sub module.
<b>Syntax</b>	<code>ip igmp snooping query-forward {all-ports   non-router-ports}</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>all-ports</b> - Configures the IGMP query forward administrative control status as all VLAN member ports. This is done to find out if there are any interested listeners in the network.</li><li>• <b>non-router-ports</b> - Configures the IGMP query forward administrative control status as non-router ports only. This is done to reduce the traffic in the network.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	non-router-ports
<b>Example</b>	<code>SEFOS(config)# ip igmp snooping query-forward all-ports</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>show ip igmp snooping globals</b> - Displays the IGMP snooping information for all VLANs or a specific VLAN.</li></ul>

---

## 34.13 ip igmp snooping version

---

<b>Command Objective</b>	This command configures the operating version of the IGMP snooping switch for a specific VLAN. The version can be set manually to execute condition specific commands.
<b>Syntax</b>	<code>ip igmp snooping version { v1  v2   v3}</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>v1</code> - Configures the version as IGMP snooping Version 1.</li><li>• <code>v2</code> - Configures the version as IGMP snooping Version 2.</li><li>• <code>v3</code> - Configures the version as IGMP snooping Version 3.</li></ul>
<b>Mode</b>	Config-VLAN Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	v3
<b>Example</b>	<code>SEFOS(config-vlan)#ip igmp snooping version v2</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp snooping</code> - Displays IGMP snooping information for all VLANs or a specific VLAN.</li><li>• <code>show ip igmp forwarding-database</code> - Displays multicast forwarding entries.</li></ul>

---

## 34.14 ip igmp snooping fast-leave

---

<b>Command Objective</b>	<p>This command enables fast leave processing and IGMP snooping for a specific VLAN. It enables IGMP snooping only for the specific VLAN, when IGMP snooping is globally disabled.</p> <p>When the fast leave feature is enabled, port information is removed from a multicast group entry immediately after fast leave message is received.</p> <p>The no form of the command disables fast leave processing for a specific VLAN.</p>
<b>Syntax</b>	<pre>ip igmp snooping fast-leave</pre> <pre>no ip igmp snooping fast-leave</pre>
<b>Mode</b>	Config-VLAN Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	Fast leave processing is disabled.
	<p><u>Note:</u> Fast leave configurations done in a VLAN, when IGMP snooping is disabled in a VLAN, will be applied only when IGMP snooping is enabled in the VLAN.</p>
<b>Example</b>	<pre>SEFOS (config-vlan)# ip igmp snooping fast-leave</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ip igmp snooping</code> - Enables IGMP snooping in the switch or a specific VLAN.</li><li>• <code>show ip igmp snooping</code> - Displays IGMP snooping information for all VLANs or a specific VLAN.</li><li>• <code>show ip igmp snooping globals</code> - Displays the global information of IGMP snooping.</li></ul>

---

## 34.15 ip igmp snooping vlan - immediate leave

---

<b>Command Objective</b>	<p>This command enables fast leave processing and IGMP snooping for a specific VLAN. It enables IGMP snooping only for the specific VLAN, when IGMP snooping is globally disabled. When the fast leave feature is enabled, port information is removed from a multicast group entry immediately after fast leave message is received. The ID of the VLAN ranges between 1 and 4094.</p> <p>The no form of the command disables fast leave processing for a specific VLAN.</p> <p>This command is a standardized implementation of the existing command <code>ip igmp snooping fast-leave</code>. Its operation is similar to the existing command.</p>
<b>Syntax</b>	<pre>ip igmp snooping vlan &lt;vlanid(1-4094)&gt; immediate-leave</pre> <pre>no ip igmp snooping vlan &lt;vlanid(1-4094)&gt; immediate-leave</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	Fast leave processing is disabled in all the VLANs.
<b>Note:</b>	Fast leave configurations done in a VLAN, when IGMP snooping is disabled in a VLAN, will be applied only when IGMP snooping is enabled in the VLAN.
<b>Example</b>	<pre>SEFOS (config)# ip igmp snooping vlan 1 immediate-leave</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li><code>ip igmp snooping</code> - Enables IGMP snooping in the switch or a specific VLAN.</li><li><code>show ip igmp snooping</code> - Displays IGMP snooping information for all VLANs or a specific VLAN.</li></ul>

---

## 34.16 ip igmp snooping querier

---

<b>Command Objective</b>	<p>This command configures the IGMP snooping switch as a querier for a specific VLAN. When configured as a querier, the switch sends IGMP query messages. The query messages will be suppressed if there are any routers in the network.</p> <p>The no form of the command configures the IGMP snooping switch as non-querier for a specific VLAN.</p>
<b>Syntax</b>	<pre>ip igmp snooping querier</pre> <pre>no ip igmp snooping querier</pre>
<b>Mode</b>	Config-VLAN Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	Non-querier
<b>Example</b>	<pre>SEFOS (config-vlan)# ip igmp snooping querier</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp snooping</code> - Displays IGMP snooping information for all VLANs or a specific VLAN.</li></ul>

---

## 34.17 ip igmp snooping query-interval

---

<b>Command Objective</b>	<p>This command sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN. The switch sends querier messages in proxy mode and proxy-reporting mode to all downstream interfaces for this time interval. The value range is between 60 to 600 seconds.</p> <p>The no form of the command sets the IGMP querier interval to default value.</p>
<b>Syntax</b>	<pre>ip igmp snooping query-interval &lt;(60 - 600) seconds&gt;  no ip igmp snooping query-interval</pre>
<b>Mode</b>	Config-VLAN Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	125 Seconds
	<p><u>Note:</u></p> <ul style="list-style-type: none"><li>• The switch must be configured as a querier for this configuration to be imposed.</li><li>• In proxy-reporting mode, general queries are sent on all downstream interfaces with this interval only if the switch is the querier.</li><li>• In proxy mode, general queries will be sent on all downstream interfaces with this interval.</li></ul>
<b>Example</b>	<pre>SEFOS (config-vlan) # ip igmp snooping query-interval 200</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp snooping</code> - Displays IGMP snooping information for all VLANs or a specific VLAN.</li></ul>

---

## 34.18 ip igmp snooping startup-query-interval

---

<b>Command Objective</b>	<p>This command sets the time interval between the general query messages sent by the IGMP snooping switch, during startup of the querier election process. This time interval ranges between 15 and 150 seconds and should be less than or equal to query interval divided by 4.</p> <p>The no form of the command sets the IGMP startup query interval to the default value.</p>
<b>Syntax</b>	<pre>ip igmp snooping startup-query-interval &lt;(15 - 150) seconds&gt;  no ip igmp snooping startup-query-interval</pre>
<b>Mode</b>	Config-VLAN Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	31 Seconds
	<p><u>Note:</u></p> <ul style="list-style-type: none"><li>• The switch should be configured as querier for the startup query interval command to produce results.</li><li>• The startup query interval should be less than or equal to one-fourth of the query interval.</li></ul>
<b>Example</b>	<pre>SEFOS(config-vlan) # ip igmp snooping startup-query- interval 100</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>ip igmp snooping query-interval</b> - Sets the time period with which the general queries are sent by the IGMP snooping switch, when configured as querier on a VLAN.</li><li>• <b>show ip igmp snooping querier</b> - Displays IGMP snooping information for all VLANs or a specific VLAN.</li><li>• <b>show ip igmp snooping</b> - Displays IGMP snooping information for all VLANs or a specific VLAN for a given context or for all the contexts.</li></ul>

---



## 34.19 ip igmp snooping startup-query-count

---

**Command Objective** This command sets the maximum number of general query messages sent out on switch startup, when the switch is configured as a querier. This value ranges from 2 to 5. Startup query messages are sent to announce the presence of the switch along with its identity. The startup query count is manually configured to change the existing count. This value ranges from 2 to 5.

The no form of the command sets the number of general query messages sent out on switch startup, when the switch is configured as a querier to default value.

---

**Syntax** `ip igmp snooping startup-query-count <2 - 5>`  
`no ip igmp snooping startup-query-count`

---

**Mode** Config-VLAN Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Default** 2

---

Note: The switch should be configured as a querier, for startup query count configuration to be effective.

---

**Example** `SEFOS (config-vlan) # ip igmp snooping startup-query-count 4`

---

**Related Command(s)**

- `ip igmp snooping querier` - Configures the IGMP snooping switch as a querier for a specific VLAN.
- `ip igmp snooping query-interval` - Sets the time period with which the general queries are sent by the IGMP snooping switch.
- `ip igmp snooping clear counters` - Clears the IGMP snooping statistics maintained for VLAN(s).
- `show ip igmp snooping` - Displays IGMP snooping information for all VLANs or a specific VLAN.

---

## 34.20 ip igmp snooping other-querier-present-interval

---

<b>Command Objective</b>	<p>This command sets the maximum time interval to decide that another querier is present in the network. This time interval ranges between 120 and 1215 seconds. Within this time interval, if the querier receives response from another querier, then the one with a higher IP address is announced as the querier for the network. The other-querier-present interval must be greater than or equal to <math>((\text{Robustness Variable} * \text{Query Interval}) + (\text{Query Response Interval}/2))</math>. Here, Robustness value is 2.</p> <p>The no form of the command resets this interval to default value.</p>
<b>Syntax</b>	<pre>ip igmp snooping other-querier-present-interval &lt;value (120-1215) seconds&gt;  no ip igmp snooping other-querier-present-interval</pre>
<b>Mode</b>	Config-VLAN Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	255 Seconds
	<p><u>Note:</u> The switch should be configured as a querier for the other-querier-present command to be effective.</p>
<b>Example</b>	<pre>SEFOS(config-vlan) # ip igmp snooping other-querier- present-interval 1215</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>ip igmp snooping querier</b> - Configures the IGMP snooping switch as a querier for a specific VLAN.</li><li>• <b>ip igmp snooping query-interval</b> - Sets the time period with which the general queries are sent by the IGMP snooping switch, when configured as querier on a VLAN.</li><li>• <b>ip igmp snooping max-response-code</b> - Sets the maximum response code inserted in general queries sent to host.</li><li>• <b>show ip igmp snooping</b> - Displays IGMP snooping information for all VLANs or a specific VLAN.</li></ul>

---

## 34.21 ip igmp snooping mrouter

---

<b>Command Objective</b>	<p>This command enables IGMP snooping and configures a list of multicast router ports for a specific VLAN, when IGMP snooping is globally enabled. This will enable IGMP snooping only for the specific VLAN, if IGMP snooping is globally disabled.</p> <p>Any IGMP message received on a switch is forwarded only on the router-ports and not on the host ports. In this manner, the IGMP snooping functionality avoids flooding of IGMP query messages from the host to the entire network.</p> <p>The no form of the command deletes the statically configured router ports for a VLAN.</p>
<b>Syntax</b>	<pre>ip igmp snooping mrouter &lt;interface-type&gt; &lt;0/a-b, 0/c, ...&gt;  no ip igmp snooping mrouter &lt;interface-type&gt; &lt;0/a-b, 0/c, ...&gt;</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>&lt;interface-type&gt;</b> - Configures list of multicast router ports for the specified type of interface. The interface can be:<ul style="list-style-type: none"><li>▪ <b>fastethernet</b> – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.</li><li>▪ <b>XL-ethernet</b> – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.</li></ul><hr/><p>Note: As of release 2.0.0.3, all interfaces are referred to as extreme-ethernet.</p><hr/><ul style="list-style-type: none"><li>▪ <b>extreme-ethernet</b> – A version of Ethernet that supports data transfer up to 10 Gigabits per second.</li><li>▪ <b>i-lan</b> – Internal LAN created on a bridge per IEEE 802.1ap.</li><li>▪ <b>port-channel</b> – Logical interface that represents an aggregator which contains several ports aggregated together.</li></ul></li><li>• <b>&lt;0/a-b, 0/c, ...&gt;</b> - Sets a list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided, for interface types internal-lan and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3.</li></ul>
<b>Mode</b>	Config-VLAN Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro

---

---

**Note:** The list of multicast router ports configured while IGMP snooping is disabled in the VLAN is applied only when the IGMP snooping is enabled in the VLAN.

---

**Example** SEFOS (config-vlan)# ip igmp snooping mrouter extreme-  
ethernet 0/1

---

**Related Command(s)**

- `ip igmp snooping` - Enables IGMP snooping in the switch or a specific VLAN.
- `show ip igmp snooping mrouter` - Displays the router ports for all VLANs or specific VLAN.
- `ip igmp snooping mrouter-port -time-out` - Configures the router port purge time-out interval for a VLAN.
- `ip igmp snooping mrouter-port-version` - Configures the operating version of the router port for a VLAN.

---

## 34.22 ip igmp snooping vlan mrouter

---

**Command Objective** This command enables IGMP snooping and configures a list of multicast router ports for a specific VLAN, if IGMP snooping is globally enabled. This will enable IGMP snooping only for the specific VLAN, if IGMP snooping is globally disabled.

Any IGMP message received on a switch is forwarded only on the router-ports and not on host ports. In this manner, the IGMP snooping functionality avoids flooding of IGMP query messages from the host to the entire network.

The no form of the command deletes the statically configured router ports for a VLAN.

This command is a standardized implementation of the existing command `ip igmp snooping mrouter`. Its operation is similar to the existing command.

---

**Syntax** `ip igmp snooping vlan <vlanid (1-4094)> mrouter <ifXtype> <0/a-b, 0/c, ...>`

`no ip igmp snooping vlan <vlanid (1-4094)> mrouter <ifXtype> <0/a-b, 0/c, ...>`

---

**Parameter Description**

- **<vlanid (1-4094)>** - Configures the VLAN for which the list of multicast router ports should be configured statically. This is a unique value that represents the specific L3 VLAN created. An L3 VLAN interface is a VLAN that is mapped to an IP interface and assigned an IP address. This value ranges from 1 to 4094.
- **<ifXtype>** - Configures the list of multicast router ports for the specified type of interface. The interface can be:
  - **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
  - **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gigabits per second.
  - **i-lan** – Internal LAN created on a bridge per IEEE 802.1ap.
  - **port-channel** – Logical interface that represents an aggregator which contains several ports aggregated together.
- **<0/a-b, 0/c, ...>** - Sets a list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided, for interface types internal-lan and port-channel. Use comma as a separator

---

without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3.

---

**Mode** Global Configuration Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

Note: The list of multicast router ports configured while IGMP snooping is disabled in the VLAN is applied only when the IGMP snooping is enabled in the VLAN.

---

**Example** SEFOS(config)# ip igmp snooping vlan 1 mrouter extreme-  
ethernet 0/1

---

**Related Command(s)**

- `ip igmp snooping` - Enables IGMP snooping in the switch or a specific VLAN.
- `show ip igmp snooping mrouter` - Displays the router ports for all VLANs or specific VLAN.
- `ip igmp snooping mrouter-port -time-out` - Configures the router port purge time-out interval for a VLAN.
- `ip igmp snooping mrouter-port-version` - Configures the operating version of the router port for a VLAN.

---

## 34.23 shutdown snooping

---

<b>Command Objective</b>	<p>This command shuts down snooping in the switch. When the user does not require the IGMP snooping module to be running, it can be shut down. When shut down, all resources acquired by the snooping module are released to the system. For the IGS feature to be functional on the switch, the 'system-control' status must be set as 'start' and the 'state' must be 'enabled'.</p> <p>The no form of the command starts and enables snooping in the switch.</p>
<b>Syntax</b>	<pre>shutdown snooping no shutdown snooping</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	Snooping is enabled.
	<p><u>Note:</u> Snooping cannot be started in the switch, if the base bridge mode is configured as transparent bridging.</p>
<b>Example</b>	<pre>SEFOS(config)# shutdown snooping</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>base bridge-mode</b> - Configures the mode in which the VLAN feature should operate on the switch.</li><li>• <b>ip igmp snooping</b> - Enables IGMP snooping in the switch or a specific VLAN.</li></ul>

---

## 34.24 debug ip igmp snooping

---

**Command Objective** This command configures the various debug and trace statements to handle error and event management available in the IGMP snooping module. The traces are enabled by passing the necessary parameters.

The no form of the command resets debug options for IGMP snooping module.

---

**Syntax**

```
debug ip igmp snooping
{[init][resources][tmr][src][grp][qry]
[vlan][pkt][fwd][mgmt][redundancy] | all } [switch
<switch_name>]
```

```
no debug ip igmp snooping
{[init][resources][tmr][src][grp][qry]
[vlan][pkt][fwd][mgmt][redundancy] | all } [switch
<switch_name>]
```

---

**Parameter Description**

- **init** - Generates Init and Shutdown trace messages at the instances when the module is initiated or shut down. The information is logged in a file.
- **resources** - Generates System Resources management trace messages when there is a change in the resource status. The information is logged in a file.
- **tmr** - Generates Timer trace messages at the instances where timers are involved. The information is logged in a file.
- **src** - Generates trace messages when source information is involved.
- **grp** - Generates trace messages when group information is involved.
- **qry** - Generates trace messages when query messages are sent or received.
- **vlan** - Generates trace messages when VLAN-related information is involved.
- **pkt** - Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets.
- **fwd** - Generates traces messages when forwarding database is involved.
- **mgmt** - Generates debug statements for management plane functionality traces.
- **redundancy** - Generates debug statements for redundancy code flow



---

traces. This trace is generated when there is a failure in redundancy processing.

- **all** - Generates all types of trace messages.
- **switch <switch\_name>** - Generates switch-related trace messages.

---

**Mode** Privileged EXEC Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Default** Debugging is disabled.

---

**Example** SEFOS# debug ip igmp snooping fwd

---

**Related Command(s)**

- **show debugging** - Displays state of each debugging option.

---

## 34.25 snooping leave-process config-level

---

<b>Command Objective</b>	This command specifies the level of configuring the leave processing mechanisms. When the switch intercepts a leave group message on a switch port, it normally sends a query to that multicast group through the same switch port. If no hosts respond to the query and no multicast routers have been discovered on the switch port, that port is removed from the multicast group.
<b>Syntax</b>	<code>snooping leave-process config-level {vlan   port}</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>vlan</code> - Configures the leave mechanism at the VLAN level. In VLAN-based leave processing mode, the fast leave functionality configurable per VLAN or normal leave configurations are available for processing leave messages.</li><li>• <code>port</code> - Configures the leave mechanism at port level. In port-based leave processing mode, the explicit host tracking functionality, the fast leave functionality, or normal leave configurable on an interface are used for processing the leave messages.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	vlan
<b>Example</b>	<code>SEFOS(config)# snooping leave-process config-level port</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ip igmp snooping leavemode</code> – Configures the port leave mode for an interface.</li><li>• <code>show ip igmp snooping globals</code> – Displays IGMP snooping information for all VLANs or a specific VLAN, for a given switch or for all switches (if switch is not specified).</li></ul>

---

## 34.26 snooping report-process config-level

---

<b>Command Objective</b>	This command sets the configuration level for report processing as non-router ports or as all ports.
<b>Syntax</b>	<code>snooping report-process config-level {non-router-ports   all-ports}</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>non-router-ports</code> - The incoming report messages are processed only in the non-router ports. Report messages received on the router ports are not processed in this configuration.</li><li>• <code>all-ports</code> - The incoming report messages are processed in all the ports inclusive of router ports.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	non-router-ports
<b>Example</b>	<pre>SEFOS(config)# snooping report-process config-level all-ports</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp snooping globals</code> - Displays the IGMP snooping information for all VLANs or a specific VLAN.</li></ul>

---

## 34.27 mvr

---

**Command Objective** This command configures the multicast VLAN feature on a port. Multicast VLAN feature is used for applications where wide-scale deployment of multicast traffic is necessary. MVLAN Registration allows a subscriber on a port to subscribe and unsubscribe to a particular multicast stream on any of the multicast VLANs. Multicast VLANs enable efficient multicast dataflow in separate M-VLANs, while normal data flows through VLANs.

The no form of this command disables the multicast VLAN feature.

This command is a standardized implementation of the existing command `ip igmp snooping multicast-vlan`. Its operation is similar to the existing command.

---

**Syntax** `mvr`

`no mvr`

---

**Mode** Global Configuration Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Default** Multicast VLAN feature is disabled.

---

**Example** `SEFOS(config)# mvr`

---

**Related Command(s)**

- `show ip igmp snooping multicast-vlan` – Displays multicast VLAN statistics in a switch and displays various profiles mapped to the multicast VLANs.
- `show ip igmp snooping globals` – Displays IGMP snooping information for all VLANs or a specific VLAN, for a given switch or for all switches (if switch is not specified).

---

## 34.28 ip igmp snooping blocked-router

---

<b>Command Objective</b>	<p>This command configures a static router port as blocked router port.</p> <p>When configured as a blocked router, the queries, PIM DVMRP, and data messages are discarded. The corresponding port entry is removed from the forwarding database. The ports to be configured as blocked router ports must not be configured as static router ports.</p> <p>The no form of the command resets the blocked router ports to normal router port.</p>
<b>Syntax</b>	<pre>ip igmp snooping blocked-router &lt;interface-type&gt; &lt;0/a-b, 0/c, ...&gt;</pre> <pre>no ip igmp snooping blocked-router &lt;interface-type&gt; &lt;0/a-b, 0/c, ...&gt;</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>&lt;interface-type&gt;</b> - Configures the type of interface to be employed on the port.<ul style="list-style-type: none"><li>▪ <b>fastethernet</b> – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.</li><li>▪ <b>XL-ethernet</b> – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.</li><li>▪ <b>extreme-ethernet</b> – A version of Ethernet that supports data transfer up to 10 Gigabits per second.</li><li>▪ <b>i-lan</b> – Internal LAN created on a bridge per IEEE 802.1ap.</li><li>▪ <b>port-channel</b> – Logical interface that represents an aggregator which contains several ports aggregated together.</li></ul></li><li>• <b>&lt;0/a-b, 0/c, ...&gt;</b> - Configures the list of router-ports to be set as blocked. The interface IDs are given as an array. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided, for interface types internal-lan and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3.</li></ul>
<b>Mode</b>	Config-VLAN Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Note:</b>	The ports to be configured as blocked router ports, must not be configured as static router ports.

---

---

**Example**

```
SEFOS (config-vlan)# ip igmp snooping blocked-router  
extreme-ethernet 0/2
```

---

**Related Command(s)**

- `show ip igmp snooping blocked-router` – Displays the blocked router ports for all VLANs or a specific VLAN, for a given switch or for all the switches (if no switch is specified).
-

## 34.29 ip igmp snooping multicast-vlan profile

---

<b>Command Objective</b>	<p>This command configures profile ID-to-VLAN mapping for multicast VLAN classification. The switch is configured with list of entries such as multicast group, multicast source, and filter mode. These entries are maintained in access profiles. Each profile is associated with a particular VLAN which is categorized as multicast VLAN. When any untagged report or leave message is received (that is, packet with no tag in a customer bridge or packet with no S-tag in a provider or 802.1ad bridge), and if the group and source address in the received packet matches any rule in this profile, then the received packet is classified to be associated to the VLAN (that is, multicast VLAN) to which the profile is mapped.</p> <p>The no form of the command removes the profile ID to VLAN mapping for multicast VLAN classification.</p>
<b>Syntax</b>	<pre>ip igmp snooping multicast-vlan profile &lt;Profile ID (0-4294967295)&gt;  no ip igmp snooping multicast-vlan profile</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>&lt;Profile ID (0-4294967295)&gt;</b> - Configures the multicast profile ID for a particular VLAN. This value ranges from 0 to 4294967295.</li></ul>
<b>Mode</b>	Config-VLAN Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	0
<b>Note:</b>	<ul style="list-style-type: none"><li>• Multicast snooping mode should be IP-based.</li><li>• This command can be executed only after creating a multicast profile and setting the action for the created profile as permit.</li><li>• The configurations done by this command will take effect only if the profile is activated.</li></ul>
<b>Example</b>	<pre>SEFOS (config-vlan)# ip igmp snooping multicast-vlan profile 1</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>ip mcast profile</b> – Creates or modifies a multicast profile.</li><li>• <b>permit</b>– Configures the action for the profile as permit.</li><li>• <b>profile active</b> – Activates the profile entry.</li><li>• <b>show ip mcast profile statistics</b> – Displays the profile statistics.</li></ul>

---

## 34.30 ip igmp snooping leavemode

<b>Command Objective</b>	This command configures the port leave mode for an interface. The mechanism to process the leave messages in the downstream is selected. The switch sends an IGMP query message to find if there is any host interested in the multicast group.
<b>Syntax</b>	<code>ip igmp snooping leavemode {exp-hosttrack   fastLeave   normaleave} [InnerVlanId &lt;short (1-4094)&gt;]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>exp-hosttrack</b> - Configures the port to use the explicit host tracking mode to process the leave messages. The decision to remove the interface is made based on the tracked host information.</li><li>• <b>fastLeave</b> - Configures the port to use the fast leave mode to process the leave messages. On receiving a leave message the interface is removed from the group registration and the leave message is sent to the router ports.</li><li>• <b>normalleave</b> - Configures the port to use the normal leave mode. The normal leave mode is applicable only for v2 hosts. When the system receives a v2 leave message, it sends a group-specific query on the interface. For v3 hosts, normal leave has no effect.</li><li>• <b>InnerVlanId &lt;short (1-4094)&gt;]</b> - Configures the inner VLAN ID. In provider bridging domain, the customer VLAN itag InnerVlanId. This value ranges from 1 to 4094.<ul style="list-style-type: none"><li>▪ If InnerVlanId is specified, multicast forwarding mode must be IP-based and enhanced mode must be enabled in the snooping system.</li><li>▪ If InnerVlanId is not specified, leave mode can be configured irrespective of multicast forwarding mode and enhanced mode status.</li></ul></li></ul>
<b>Mode</b>	Interface Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	exp-host track/fastLeave/normalleave - Normalleave
<b>Note:</b>	The leave process configuration level has to be port.
<b>Example</b>	<pre>SEFOS(config-if)# ip igmp snooping leavemode fastLeave InnerVlanId 1</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>snooping leave-process config-level</b> – Specifies the level of configuring the leave processing mechanisms.</li><li>• <b>ip igmp snooping enhanced-mode</b> – Enables or disables snooping</li></ul>



---

system enhanced mode in the switch.

- **snooping multicast-forwarding-mode** – Specifies the snooping multicast forwarding mode.
  - **show ip igmp snooping port-cfg** – ion information for all iDisplays IGS port configuration information for all inner VLANs, a specific inner VLAN ID, or a given switch.
  - **show ip igmp snooping multicast-receivers** – Displays IGMP multicast host information for all VLANs, a specific VLAN, or specific VLAN and group address, for a given switch or for all switches (if no switch is specified).
-

## 34.31 ip igmp snooping ratelimit

---

<b>Command Objective</b>	<p>This command configures the rate limit for a downstream interface in units of the number of IGMP packets per second. The switch allows configuring the maximum rate of IGMP reports incoming for a port. The IGMP rate limiting eliminates the bursts or attacks from specific physical port. It prevents the exhaustion of system resources.</p> <p>The no form of the command resets the rate limit to default value for an interface. By default, the rate limit will hold the maximum value supported by an unsigned integer and will not rate limit any IGMP packets.</p>
<b>Syntax</b>	<pre>ip igmp snooping ratelimit &lt;integer&gt; [InnerVlanId &lt;short (1-4094)&gt;]  no ip igmp snooping ratelimit [InnerVlanId &lt;short (1-4094)&gt;]</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>ratelimit &lt;integer&gt;</b> - Configures the ratelimit value for a downstream interface in units of the number of IGMP packets per second.</li><li>• <b>InnerVlanId &lt;short (1-4094)&gt;</b> - Configures the ratelimit value for inner VLAN identifier. This value ranges from 1 to 4094. If InnerVlanId is specified, then enhanced mode should be enabled. If InnerVlanId is not specified, enhanced mode need not be enabled.</li></ul>
<b>Mode</b>	Interface Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	rate limit is 4294967295.
<b>Note:</b>	<ul style="list-style-type: none"><li>• The actual rate supported will depend on what the system can support.</li><li>• The IGMP snooping filter must be enabled for this configuration to have the effect.</li><li>• Even without enabling IGMP snooping filter, control plane data structure update takes place. But the benefits can be realized only when IGMP snooping filter is enabled.</li></ul>
<b>Example</b>	<pre>SEFOS(config-if)# ip igmp snooping ratelimit 100 InnerVlanId 1</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>ip igmp snooping enhanced-mode</b> – Enables or disables snooping system enhanced mode in the switch.</li><li>• <b>ip igmp snooping filter</b> – Enables the IGMP snooping filter.</li></ul>

---

- 
- **show ip igmp snooping port-cfg** – Displays IGS port configuration information for all inner VLANs, a specific inner VLAN ID, or a given switch.
  - **ip mcast profile** – Creates or modifies a multicast profile.
  - **profile active** – Activates the profile entry.
-

## 34.32 ip igmp snooping limit

<b>Command Objective</b>	<p>This command configures the maximum limit type for an interface. The maximum limit is the number of unique registrations for a channel or group.</p> <p>The no form of the command configures the maximum limit type as none for an interface.</p>
<b>Syntax</b>	<pre>ip igmp snooping limit { channels   groups } &lt;interger32&gt; [InnerVlanId &lt;short (1-4094)&gt;]  no ip igmp snooping limit [InnerVlanId &lt;short (1-4094)&gt;]</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>Channels</b> - Configures the snooping maximum limit as channels (group or source). Channel limit is applied for IGMPv3 to include and allow reports.</li><li>• <b>Groups</b> - Configures the snooping maximum limit as groups. Group limit is applied for all IGMP reports.</li><li>• <b>&lt;interger32&gt;</b> - Configures the snooping maximum limit. The maximum limit is the number of unique registrations for a channel or group. This value ranges from 0 to 4294967295.</li><li>• <b>InnerVlanId &lt;short (1-4094)&gt;</b> - Configures the maximum limit type for the Inner VLAN identifier. This value ranges from 1 to 4094. then enhanced mode should be enabled. If InnerVlanId is not specified, enhanced mode need not be enabled</li></ul>
<b>Mode</b>	Interface Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	The limit is set as 0 so that no limiting is done.
	<p><u>Note:</u></p> <ul style="list-style-type: none"><li>• The IGMP snooping filter must be enabled for this configuration to have the effect.</li><li>• Even without enabling IGMP snooping filter, control plane data structure update takes place. But the benefits can be realized only when IGMP snooping filter is enabled.</li></ul>
<b>Example</b>	<pre>SEFOS(config-if)# ip igmp snooping limit groups 10 InnerVlanId 1</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>ip igmp snooping enhanced-mode</b> – Enables or disables snooping system enhanced mode in the switch.</li><li>• <b>ip igmp snooping filter</b> – Enables the IGMP snooping filter.</li></ul>

- 
- **show ip igmp snooping port-cfg** – Displays IGS port configuration information for all inner VLANs, a specific inner VLAN ID, or a given switch.
  - **ip mcast profile** – Creates or modifies a multicast profile.
  - **profile active** – Activates the profile entry.
  - **ip igmp filter** - Creates a multicast filter profile index for an interface.
  - **ip igmp max-groups** - Configures the maximum number of multicast groups that can be learned on the interface.
-

## 34.33 ip igmp snooping filter-profileId

<b>Command Objective</b>	<p>This command configures the multicast profile index for a downstream interface. This profile contains a set of allowed or denied rules to be applied for the IGMP packets received through this downstream interface.</p> <p>The no form of the command resets the multicast profile index to default value.</p>
<b>Syntax</b>	<pre>ip igmp snooping filter-profileId &lt;integer&gt; [InnerVlanId &lt;short (1-4094)&gt;]  no ip igmp snooping filter-profileId [InnerVlanId &lt;short (1-4094)&gt;]</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li><b>filter-profileId &lt;integer&gt;</b> - Configures the multicast filter profile index for a downstream interface.</li><li><b>InnerVlanId &lt;short (1-4094)&gt;</b> - Configures multicast filter profile index for the Inner VLAN identifier. This value ranges from 1 to 4094. If InnerVlanId is specified, then enhanced mode should be enabled. If InnerVlanId is not specified, enhanced mode need not be enabled.</li></ul>
<b>Mode</b>	Interface Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	The profile ID is 0.
<b>Note:</b>	<ul style="list-style-type: none"><li>The IGMP snooping filter must be enabled for this configuration to have the effect.</li><li>Even without enabling IGMP snooping filter, control plane data structure update takes place. But the benefits can be realized only when IGMP snooping filter is enabled.</li><li>IGMP Snooping Multicast forwarding mode must be IP-based.</li></ul>
<b>Example</b>	<pre>SEFOS(config-if)# ip igmp snooping filter-profileId 2 InnerVlanId 1</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li><b>ip igmp snooping enhanced-mode</b> – Enables or disables snooping system enhanced mode in the switch.</li><li><b>ip igmp snooping filter</b> – Enables the IGMP snooping filter.</li><li><b>snooping multicast-forwarding-mode ip</b> - Sets the snooping multicast forwarding mode as IP address based.</li></ul>

- 
- **show ip igmp snooping port-cfg** – Displays IGS port configuration information for all inner VLANs, a specific inner VLAN ID, or a given switch.
  - **ip mcast profile** – Creates or modifies a multicast profile.
  - **profile active** – Activates the profile entry.
  - **show ip mcast profile statistics** – Displays the profile statistics.
  - **ip igmp filter** - Creates a multicast filter profile index for an interface.
-

## 34.34 ip igmp snooping proxy

---

<b>Command Objective</b>	<p>This command enables proxy in the IGMP snooping switch. In proxy mode, the switch acts as a querier for all downstream interfaces and a host for all upstream interfaces. The switch sends general query to all downstream interfaces at the query interval and collects information about the member ports. The proxy sends current consolidated report and state change report to upstream interfaces.</p> <p>The no form of the command disables proxy in the IGMP snooping switch.</p>
<b>Syntax</b>	<pre>ip igmp snooping proxy  no ip igmp snooping proxy</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	The proxy is disabled in the IGMP snooping switch.
	<p><u>Note:</u> Proxy can be enabled in the IGMP snooping switch only if the proxy-reporting is disabled in the snooping switch.</p>
<b>Example</b>	<pre>SEFOS(config)# ip igmp snooping proxy</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>no ip igmp snooping proxy-reporting</b> – Disables proxy-reporting in the IGMP snooping switch.</li><li>• <b>show ip igmp snooping globals</b> – Displays IGMP snooping information for all VLANs or a specific VLAN, for a given switch or for all switches (if switch is not specified).</li></ul>

---



## 34.35 ip igmp snooping max-response-code

---

**Command Objective** This command sets the maximum response code inserted in general queries sent to host. The unit of the response code is tenth of second. This value ranges from 0 to 255.

The no form of the command sets the query response code to default value.

---

**Syntax** `ip igmp snooping max-response-code <(0 - 255)>`

`no ip igmp snooping max-response-code`

---

**Mode** Config-VLAN Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Default** 100

---

**Example** `SEFOS(config-vlan)# ip igmp snooping max-response-code 10`

---

**Related Command(s)**

- `show ip igmp snooping` - Displays IGMP snooping information for all VLANs or a specific VLAN.

---

## 34.36 ip igmp snooping mrouter-port –time-out

---

<b>Command Objective</b>	<p>This command configures the router port purge time-out interval for a VLAN. The time interval after which the proxy assumes there are no v1 or v2 routers present on the upstream port. While the older querier timer is running, the proxy replies to all the queries with consolidated v1 or v2 reports. When the timer expires, if the v2 or v3 queriers are not present and the port is dynamically learned, the port is purged. If the port is static router port, the proxy replies to all queries with new version of v2/v3 consolidated reports.</p> <p>The no form of the command resets the router port purge time-out interval to default, for a VLAN.</p>
<b>Syntax</b>	<pre>ip igmp snooping mrouter-port &lt;ifXtype&gt; &lt;iface_list&gt; time-out &lt;short(60-600)&gt;</pre> <pre>no ip igmp snooping mrouter-port &lt;interface-type&gt; &lt;0/a-b, 0/c, ...&gt;</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>&lt;ifXtype&gt; / &lt;interface-type&gt;</b> - Configures the purge time-out interval for the specified type of interface. The interface can be:<ul style="list-style-type: none"><li>▪ <b>fastethernet</b> – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.</li><li>▪ <b>XL-ethernet</b> – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.</li><li>▪ <b>extreme-ethernet</b> – A version of Ethernet that supports data transfer up to 10 Gigabits per second.</li><li>▪ <b>i-lan</b> – Internal LAN created on a bridge per IEEE 802.1ap.</li><li>▪ <b>port-channel</b> – Logical interface that represents an aggregator which contains several ports aggregated together.</li></ul></li><li>• <b>&lt;iface_list&gt; / &lt;0/a-b, 0/c, ...&gt;</b> - Configures the list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided, for interface types internal-lan and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3.</li><li>• <b>time-out &lt;short(60-600)&gt;</b> - Configures the router port purge time-out interval. This value ranges from 60 to 600 seconds.</li></ul>
<b>Mode</b>	Config-VLAN Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro

---

---

**Default**                      time-out - 125 seconds

---

Note:                      The router ports must be statically configured for the VLAN.

---

**Example**                      SEFOS(config-vlan)# ip igmp snooping mrouter-port extreme-  
   ethernet 0/1 time-out 150

---

**Related Command(s)**

- `ip igmp snooping mrouter` – Statically configures the router ports for a VLAN.
- `show ip igmp snooping mrouter detail`– Displays detailed information about the router ports.

---

## 34.37 ip igmp snooping mrouter-port-version

---

**Command Objective**

This command configures the operating version of IGMP PROXY on the upstream router port for a VLAN.

The no form of the command resets the operating version of the IGMP PROXY on the upstream router port to its default operating version.

---

**Syntax**

```
ip igmp snooping mrouter-port <ifXtype> <iface_list>
version {v1 | v2 | v3}
```

```
no ip igmp snooping mrouter-port <ifXtype> <iface_list>
version
```

---

**Parameter Description**

- **<ifXtype>** - Configures the operating version of IGMP PROXY for the specified type of interface. The interface can be:
  - **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
  - **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gigabits per second.
  - **i-lan / internal-lan** – Internal LAN created on a bridge per IEEE 802.1ap.
  - **port-channel** – Logical interface that represents an aggregator which contains several ports aggregated together.
- **<iface\_list>** - Configures the operating version of IGMP PROXY for the list of multicast router ports of the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided, for interface types internal-lan and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3.
- **Version** - Configures the operating version of the IGMP snooping.
  - **v1** – IGMP snooping Version 1
  - **v2** – IGMP snooping Version 2
  - **v3** – IGMP snooping Version 3

---

**Mode**

Config-VLAN Mode

---

**Package**

Workgroup, Enterprise, Metro\_E, and Metro

---

---

**Default** v3

---

Note: The router ports must be statically configured for the VLAN.

---

**Example** SEFOS(config-vlan)# ip igmp snooping mrouter-port extreme-  
ethernet 0/1 version v1

---

**Related Command(s)**

- `ip igmp snooping mrouter` – Statically configures the router ports for a VLAN.
- `show ip igmp snooping mrouter detail` – Displays detailed information about the router ports.

---

## 34.38 show ip igmp snooping mrouter

---

**Command Objective** This command displays the router ports for all VLANs or a specific VLAN for a given switch or for all the switches (if no switch is specified). The interface details and the corresponding port number along with its type (static or dynamic) are displayed.

---

**Syntax** `show ip igmp snooping mrouter [Vlan <vlan-id/vfi-id>]  
[detail]`

---

**Parameter Description**

- **vlan <vlan-id/vfi-id>** - Displays the router ports for the specified VLAN / VFI ID. This value ranges from 1 to 65535.
  - **<vlan -id>** - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.
  - **<vfi-id>** - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.

---

Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.

Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.

Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.

---

- **detail** - Displays detailed information about the router ports.

---

**Mode** Privileged EXEC Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Example** **Single Instance**

```
SEFOS# show ip igmp snooping mrouter
Vlan   Ports
-----
1      Ex0/1(dynamic), Ex0/2(static)
2      Ex0/1(static), Ex0/2(dynamic)
```

---

---

## Multiple Instance

```
SEFOS# show ip igmp snooping mrouter
```

```
Switch cust1
```

```
Vlan    Ports
```

```
-----
```

```
1 Ex0/1(static)
```

```
2 Ex0/1(static)
```

```
Switch cust2
```

```
Vlan    Ports
```

```
-----
```

```
1 Ex0/9(static)
```

```
2 Ex0/9(static)
```

---

### Related Command(s)

- `ip igmp snooping mrouter-time-out / ip igmp querier-timeout` - Sets the IGMP snooping router port purge time-out interval.
  - `ip igmp snooping mrouter` - Statically configures the router ports for a VLAN.
  - `ip igmp snooping mrouter-port -time-out` - Configures the router port purge time-out interval for a VLAN.
  - `ip igmp snooping mrouter-port-version` - Configures the operating version of the router port for a VLAN.
-

## 34.39 show ip igmp snooping mrouter - Redundancy

---

<b>Command Objective</b>	This command displays the router ports for all VLANs or a specific VLAN for a given switch or for all switches (if no switch is specified).
<b>Syntax</b>	<code>show ip igmp snooping mrouter [Vlan &lt;vlan-id/vfi-id&gt;] [redundancy] [detail] [switch &lt;switch_name&gt;]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>vlan &lt;vlan-id/vfi-id&gt;</b> - Displays the router ports for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.</li></ul><hr/><p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p><p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p><p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p><hr/></li><li>• <b>redundancy</b> - Displays the synced messages.</li><li>• <b>detail</b> - Displays detailed information about the router ports.</li><li>• <b>switch &lt;switch_name&gt;</b> - Displays the specified context. This value represents unique name of the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<pre>SEFOS# show ip igmp snooping mrouter redundancy Igs Redundancy Vlan Sync Data for Vlan 1 Vlan Router Port List</pre>

---



---

```
Vlan    Ports
-----  -----
      1  Ex0/1(dynamic), Ex0/3(dynamic)
IGMP Router Port List
Vlan    IGMP Ports
-----  -----
      1  Ex0/1(dynamic)
```

---

**Related Command(s)**

- **ip igmp snooping mrouter** - Statically configures the router ports for a VLAN.
  - **ip igmp snooping mrouter-port -time-out** - Configures the router port purge time-out interval for a VLAN.
  - **ip igmp snooping mrouter-port-version** - Configures the operating version of the router port for a VLAN.
-

## 34.40 show ip igmp snooping globals

---

<b>Command Objective</b>	This command displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switches (if switch is not specified).
<b>Syntax</b>	<b>show ip igmp snooping globals</b>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<p><b>Single Instance</b></p> <pre>SEFOS# show ip igmp snooping globals Snooping Configuration -----  IGMP Snooping globally enabled IGMP Snooping is operationally enabled IGMP Snooping Enhanced mode is disabled Transmit Query on Topology Change globally disabled Multicast forwarding mode is MAC based Proxy globally disabled Proxy reporting globally enabled Filter is disabled Router port purge interval is 125 seconds Port purge interval is 260 seconds Report forward interval is 5 seconds Group specific query interval is 2 seconds Reports are forwarded on router ports Group specific query retry count is 2 Multicast VLAN disabled Leave config level is Vlan based</pre> <p><b>Multiple Instance</b></p> <pre>SEFOS# show ip igmp snooping globals Switch default Snooping Configuration -----</pre>

---

---

IGMP Snooping globally enabled  
IGMP Snooping is operationally enabled  
IGMP Snooping Enhanced mode is disabled  
Transmit Query on Topology Change globally disabled  
Multicast forwarding mode is MAC based  
Proxy globally disabled  
Proxy reporting globally enabled  
Filter is disabled  
Router port purge interval is 125 seconds  
Port purge interval is 260 seconds  
Report forward interval is 5 seconds  
Group specific query interval is 2 seconds  
Reports are forwarded on router ports  
Group specific query retry count is 2  
Multicast VLAN disabled  
Leave config level is Vlan based

---

**Related Command(s)**

- **ip igmp snooping** - Enables IGMP snooping in the switch or a specific VLAN.
  - **ip igmp snooping proxy-reporting** - Enables proxy-reporting in the IGMP snooping switch.
  - **snooping multicast-forwarding-mode** - Specifies the forwarding mode (IP-based or MAC-based) that will be effective on switch restart.
  - **ip igmp snooping mrouter-port -time-out / ip igmp querier-timeout** - Sets the IGMP snooping router port purge time-out interval.
  - **ip igmp snooping port-purge-interval / ip igmp snooping source-only learning age-timer** - Configures the IGMP snooping port purge time interval.
  - **ip igmp snooping report-suppression interval** - Sets the IGMP report-suppression interval.
  - **ip igmp snooping retry-count** - Sets the maximum number of group-specific queries sent on a port on reception of a IGMPV2 leave message.
  - **ip igmp snooping version** - Specifies the IGMP snooping operating mode of the switch.
  - **ip igmp snooping report-forward** - Specifies if IGMP reports must be forwarded on all ports or router ports of a VLAN.
-

- 
- **snooping leave-process config-level** - Specifies the level of configuring the leave processing mechanisms.
  - **ip igmp snooping enhanced-mode** - Enables or disables snooping system enhanced mode in the switch.
  - **ip igmp snooping multicast-vlan** - Enables or disables the multicast VLAN feature.
  - **mvr** - Enables the multicast VLAN feature. This command is applicable only for the code using industry standard commands.
  - **ip igmp snooping filter** - Enables the IGMP snooping filter.
  - **ip igmp snooping proxy** – Enables proxy in the IGMP snooping switch.
  - **ip igmp snooping send-query** - Configures the IGMP general query transmission feature.
-

## 34.41 show ip igmp snooping

<b>Command Objective</b>	This command displays IGMP snooping information for all VLANs or a specific VLAN for a given context or for all the contexts (if no switch is specified).
<b>Syntax</b>	<code>show ip igmp snooping [Vlan &lt;vlan-id/vfi-id&gt;]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>Vlan &lt;vlan-id/vfi-id&gt;</b> - Displays IGMP snooping information for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.</li></ul></li></ul> <p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p> <p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p> <p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	Single Instance  <pre>SEFOS# show ip igmp snooping vlan 1 Snooping VLAN Configuration for the VLAN 1 IGMP Snooping enabled IGMP configured version is V3 Fast leave is disabled Snooping switch is acting as Non-Querier Query interval is 125 seconds Port Purge Interval is 260 seconds</pre>

---

Max Response Code is 100, Time is 10 seconds

#### Multiple Instance

**SEFOS# show ip igmp snooping**

Switch default

Snooping VLAN Configuration for the VLAN 1

IGMP Snooping enabled

IGMP configured version is V3

Fast leave is disabled

Snooping switch is configured as Querier

Snooping switch is acting as Non-Querier

Query interval is 125 seconds

Port Purge Interval is 260 seconds

Max Response Code is 100, Time is 10 seconds

---

#### Related Command(s)

- **ip igmp snooping** - Enables IGMP snooping in the switch or a specific VLAN.
  - **ip igmp snooping version** - Specifies the IGMP snooping operating mode of switch.
  - **ip igmp snooping port-purge-interval / ip igmp snooping source-only learning age-timer** - Configures the IGMP snooping port purge time interval.
  - **ip igmp snooping fast-leave / ip igmp snooping vlan - immediate leave** - Enables fast leave processing and IGMP snooping for a specific VLAN.
  - **ip igmp snooping querier** - Configures the IGMP snooping switch as a querier for a specific VLAN.
  - **ip igmp snooping query-interval** - Sets the time period with which the general queries are sent by the IGMP snooping switch, when configured as querier on a VLAN.
  - **ip igmp snooping max-response-code** - Sets the maximum response code inserted in general queries sent to host.
-

## 34.42 show ip igmp snooping - Redundancy

---

<b>Command Objective</b>	This command displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switches (if no switch is specified).
<b>Syntax</b>	<code>show ip igmp snooping [Vlan &lt;vlan-id/vfi-id&gt;] [redundancy] [switch &lt;switch_name&gt;]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>vlan &lt;vlan-id/vfi-id&gt;</b> - Displays IGMP snooping information for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.</li></ul><p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p><p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p><p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p></li><li>• <b>redundancy</b> - Displays the synced messages.</li><li>• <b>switch &lt;switch_name&gt;</b> - Displays the specified context. This value represents unique name of the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<pre>SEFOS# show ip igmp snooping redundancy IGMP Snooping VLAN Configuration for VLAN 1 IGMP snooping switch is acting as Non-Querier IGMP current operating version is V1</pre>

---

---

**Related Command(s)**

- **ip igmp snooping** - Enables IGMP snooping in the switch or a specific VLAN.
  - **ip igmp snooping version** - Specifies the IGMP snooping operating mode of switch.
  - **ip igmp snooping fast-leave / ip igmp snooping vlan - immediate leave** - Enables fast leave processing and IGMP snooping for a specific VLAN.
  - **ip igmp snooping querier** - Configures the IGMP snooping switch as a querier for a specific VLAN.
  - **ip igmp snooping query-interval** - Sets the time period with which the general queries are sent by the IGMP snooping switch, when configured as querier on a VLAN.
-



## 34.43 show ip igmp snooping groups

---

<b>Command Objective</b>	This command displays IGMP group information for all VLANs, a specific VLAN, or specific VLAN and group address for a given switch or for all switch (if no switch is specified) . It also displays the information for static, dynamic, or both types of multicast entries.
<b>Syntax</b>	<code>show ip igmp snooping groups [Vlan &lt;vlan-id/vfi-id&gt; [Group &lt;Address&gt;]] [{static   dynamic}]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>vlan &lt;vlan-id/vfi-id&gt;</b> - Displays IGMP snooping group information for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.</li></ul><hr/><p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p><p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p><p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p><hr/></li><li>• <b>Group &lt;Address&gt;</b> - Displays the group address of the VLAN ID.</li><li>• <b>static</b> - Displays only static multicast entries.</li><li>• <b>dynamic</b> - Displays only dynamic multicast entries. If not specified, both static and dynamic entries are displayed.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<b>Single Instance</b>  <code>/* IP based */</code>

---

---

**SEFOS# show ip igmp snooping groups**

IGMP Snooping Group information

-----  
VLAN ID:2 Group Address: 227.1.1.1  
Filter Mode: EXCLUDE  
Exclude sources: None  
V1/V2 Receiver Ports:  
    Ex0/4  
V3 Receiver Ports:  
    Port Number: Ex0/2  
        Include sources: None  
        Exclude sources:  
            12.0.0.10, 12.0.0.20  
    Port Number: Ex0/3  
        Include sources: None  
        Exclude sources:  
            12.0.0.40, 12.0.0.30

**/\* MAC based \*/**

**SEFOS# show ip igmp snooping groups**

IGMP Snooping Group information

-----  
VLAN ID:2 Group Address: 227.1.1.1  
Filter Mode: EXCLUDE  
Exclude sources: None  
Receiver Ports:  
Ex0/2, Ex0/3, Ex0/4, Ex0/5

**Multiple Instance**

**SEFOS# show ip igmp snooping groups**

Switch cust1

Snooping Group information

-----  
VLAN ID:2 Group Address: 227.2.2.2  
Filter Mode: EXCLUDE  
Exclude sources: None  
Receiver Ports:

---

---

Ex0/3, Ex0/5, Ex0/6

Switch cust2

Snooping Group information

-----  
VLAN ID:2 Group Address: 227.2.2.2

Filter Mode: EXCLUDE

Exclude sources: None

Receiver Ports:

Ex0/10

**/\* IP based \*/**

**SEFOS# show ip igmp snooping groups static**

IGMP Snooping Group information

-----  
Snooping Group information

-----  
Outer-VLAN ID:1 Group Address: 225.3.2.2 Inner-VLAN ID:0

Filter Mode: INCLUDE

Include sources: None

Outer-VLAN ID:1 Group Address: 233.3.2.2 Inner-VLAN ID:0

Filter Mode: INCLUDE

Include sources: None

Total Num of Group Addresses [2]

**/\* MAC based \*/**

**SEFOS# show ip igmp snooping groups static**

IGMP Snooping Group information

-----  
Snooping Group information

-----  
Outer-VLAN ID:1 Group Address: 225.3.2.2 Inner-VLAN ID:0

Filter Mode: INCLUDE

Include sources: None

Outer-VLAN ID:1 Group Address: 233.3.2.2 Inner-VLAN ID:0

Filter Mode: INCLUDE

Include sources: None

Total Num of Group Addresses [2]

---

---

For dynamic

**/\* IP based \*/**

**SEFOS# show ip igmp snooping groups dynamic**

Snooping Group information

-----  
Outer-VLAN ID:2 Group Address: 227.1.1.1 Inner-VLAN ID:0

Filter Mode: EXCLUDE

Exclude sources: None

ASM Receiver Ports:

Ex0/2

Outer-VLAN ID:2 Group Address: 227.2.2.2 Inner-VLAN ID:0

Filter Mode: EXCLUDE

Exclude sources: None

ASM Receiver Ports:

Ex0/3

Total Num of Group Addresses [2]

**/\* MAC based \*/**

**SEFOS# show ip igmp snooping groups dynamic**

Snooping Group information

-----  
Outer-VLAN ID:2 Group Address: 227.1.1.1 Inner-VLAN ID:0

Filter Mode: EXCLUDE

Exclude sources: None

ASM Receiver Ports:

Ex0/2

Outer-VLAN ID:2 Group Address: 227.2.2.2 Inner-VLAN ID:0

Filter Mode: EXCLUDE

Exclude sources: None

ASM Receiver Ports:

Ex0/3

---

**Related Command(s)**

- **ip igmp snooping static-group** - Configures IGMP snooping static multicast for VLAN(s)
-

## 34.44 show ip igmp snooping forwarding-database

---

<b>Command Objective</b>	This command displays multicast forwarding entries for all VLANs or a specific VLAN, for a given switch or for all switches (if no switch is specified). It also displays the information for static, dynamic, or both types of multicast entries.
<b>Syntax</b>	<code>show ip igmp snooping forwarding-database [Vlan &lt;vlan-id/vfi-id&gt;] [{static   dynamic}]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>Vlan &lt;vlan-id/vfi-id&gt;</b> - Displays multicast forwarding entries for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.</li></ul><hr/><p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p><p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p><p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p><hr/></li><li>• <b>Static</b> - Display the static multicast forwarding entries.</li><li>• <b>Dynamic</b> - Display the dynamic multicast forwarding entries. If not specified, both static and dynamic entries are displayed.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<p><b>Single Instance</b></p> <pre>/* IP based */  SEFOS# show ip igmp snooping forwarding-database static Vlan Source Address Group Address Ports</pre>

---

---

```

2      12.0.0.10      227.1.1.1 Ex0/1, Ex0/3, Ex0/4
2      12.0.0.20      227.1.1.1 Ex0/1, Ex0/3, Ex0/4
2      12.0.0.30      227.1.1.1 Ex0/1, Ex0/2, Ex0/4
2      12.0.0.40      227.1.1.1 Ex0/1, Ex0/2, Ex0/

```

**/\* MAC based \*/**

**SEFOS# show ip igmp snooping forwarding-database**

```

Vlan  MAC-Address          Ports
----  -
2     01:00:5e:01:01:01     Ex0/2, Ex0/3, Ex0/4, Ex0/5
2     01:00:5e:02:02:02     Ex0/2, Ex0/3

```

**Multiple Instance**

**SEFOS# show ip igmp snooping forwarding-database static**

Switch cust1

```

Vlan  MAC-Address          Ports
----  -
2     01:00:5e:02:02:02     Ex0/2, Ex0/3, Ex0/5, Ex0/6

```

Switch cust2

```

Vlan  MAC-Address          Ports
----  -
2     01:00:5e:02:02:02     Ex0/9, Ex0/10

```

---

**Related Command(s)**

- **ip igmp snooping** - Enables IGMP snooping in the switch or a specific VLAN.
  - **ip igmp snooping proxy-reporting** – Enables proxy-reporting in the IGMP snooping switch.
  - **ip igmp snooping version** - Configures the operating version of the IGMP snooping switch for a specific VLAN.
  - **ip igmp snooping static-group** - Configures IGMP snooping static multicast for VLAN(s). By default, both static and dynamic entries are displayed.
-

## 34.45 show ip igmp snooping forwarding-database - Redundancy

<b>Command Objective</b>	This command displays multicast forwarding entries for all VLANs or a specific VLAN, for a given switch or for all switches (if no switch is specified). It also displays the information for static, dynamic, or both types of multicast entries.
<b>Syntax</b>	<pre>show ip igmp snooping forwarding-database [Vlan &lt;vlan-id/vfi-id&gt;] [{static   dynamic}] [redundancy]</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>vlan &lt;vlan-id/vfi-id&gt;</b> - Displays multicast forwarding entries for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.</li></ul><p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p><p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p><p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p></li><li>• <b>static</b> - Display the static multicast forwarding entries.</li><li>• <b>dynamic</b> - Display the dynamic multicast forwarding entries. If not specified, both static and dynamic entries are displayed.</li><li>• <b>redundancy</b> - Displays the synced messages.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<pre>SEFOS# show ip igmp snooping forwarding-database redundancy  Igs Redundancy Multicast Group Info Sync Data</pre>

---

Vlan	Group Address	Ports
----	-----	-----
1	224.1.1.1	Ex0/2, Ex0/3
1	224.1.2.3	Ex0/1, Ex0/3

---

**Related Command(s)**

- **ip igmp snooping** - Enables IGMP snooping in the switch or a specific VLAN.
  - **ip igmp snooping proxy-reporting** – Enables proxy-reporting in the IGMP snooping switch.
  - **ip igmp snooping version** - Configures the operating version of the IGMP snooping switch for a specific VLAN.
  - **ip igmp snooping static-group** - Configures IGMP snooping static multicast for VLAN(s). By default, both static and dynamic entries are displayed.
-



## 34.46 show ip igmp snooping statistics

<b>Command Objective</b>	This command displays IGMP snooping statistics for all VLANs or a specific VLAN for a given switch or for all switches (if no switch is specified).
<b>Syntax</b>	<code>show ip igmp snooping statistics [Vlan &lt;vlan-id/vfi-id&gt;]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>Vlan &lt;vlan-id/vfi-id&gt;</b> - Displays IGMP snooping statistics for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.</li></ul></li></ul> <p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p> <p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p> <p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<p><b>Single Instance</b></p> <pre>SEFOS# show ip igmp snooping statistics IGMP Snooping Statistics for VLAN 1   IGMP Snooping General queries received : 3   IGMP Snooping Group specific queries received : 0   IGMP Snooping Group and source specific queries received : 0   IGMP Snooping V1/V2 reports received : 10   IGMP Snooping V3 reports received : 0</pre>

---

```
IGMP Snooping V3 IS_INCLUDE messages received : 0
IGMP Snooping V3 IS_EXCLUDE messages received : 0
IGMP Snooping V3 TO_INCLUDE messages received : 0
IGMP Snooping V3 TO_EXCLUDE messages received : 0
IGMP Snooping V3 ALLOW messages received : 0
IGMP Snooping V3 Block messages received : 0
IGMP Snooping V2 Leave messages received : 0
IGMP Snooping General queries transmitted : 0
IGMP Snooping Group specific queries transmitted : 2
IGMP Snooping V1/V2 reports transmitted : 0
IGMP Snooping V3 reports transmitted : 3
IGMP Snooping V2 leaves transmitted : 0
IGMP Snooping Packets dropped : 1
```

### **Multiple Instance**

#### **SEFOS# show ip igmp snooping statistics**

Switch cust1

Snooping Statistics for VLAN 1

General queries received : 0

Group specific queries received : 0

Group and source specific queries received : 0

ASM reports received : 20

SSM reports received : 0

IS\_INCLUDE messages received : 0

IS\_EXCLUDE messages received : 0

TO\_INCLUDE messages received : 0

TO\_EXCLUDE messages received : 0

ALLOW messages received : 0

Block messages received : 0

Leave messages received : 0

General queries transmitted : 0

Group specific queries transmitted : 0

ASM reports transmitted : 1

SSM reports transmitted : 0

Leaves transmitted : 0

Packets dropped : 0

Snooping Statistics for VLAN 2

---

---

General queries received : 0  
Group specific queries received : 0  
Group and source specific queries received : 0  
ASM reports received : 19  
SSM reports received : 18  
IS\_INCLUDE messages received : 0  
IS\_EXCLUDE messages received : 0  
TO\_INCLUDE messages received : 0  
TO\_EXCLUDE messages received : 0  
ALLOW messages received : 0  
Block messages received : 0  
Leave messages received : 0  
General queries transmitted : 0  
Group specific queries transmitted : 0  
ASM reports transmitted : 2  
SSM reports transmitted : 0  
Leaves transmitted : 0  
Packets dropped : 0

Switch cust2

Snooping Statistics for VLAN 1

General queries received : 0  
Group specific queries received : 0  
Group and source specific queries received : 0  
ASM reports received : 0  
SSM reports received : 0  
IS\_INCLUDE messages received : 0  
IS\_EXCLUDE messages received : 0  
TO\_INCLUDE messages received : 0  
TO\_EXCLUDE messages received : 0  
ALLOW messages received : 0  
Block messages received : 0  
Leave messages received : 0  
General queries transmitted : 0  
Group specific queries transmitted : 0  
ASM reports transmitted : 0  
SSM reports transmitted : 0  
Leaves transmitted : 0

---

---

```
Packets dropped : 0
Snooping Statistics for VLAN 2
  General queries received : 0
  Group specific queries received : 0
  Group and source specific queries received : 0
  ASM reports received : 0
  SSM reports received : 0
  IS_INCLUDE messages received : 0
  IS_EXCLUDE messages received : 0
  TO_INCLUDE messages received : 0
  TO_EXCLUDE messages received : 0
  ALLOW messages received : 0
  Block messages received : 0
  Leave messages received : 0
  General queries transmitted : 0
  Group specific queries transmitted : 0
  ASM reports transmitted : 0
  SSM reports transmitted : 0
  Leaves transmitted : 0
  Packets dropped : 0
```

---

**Related Command(s)**

- **ip igmp snooping** - Enables IGMP snooping in the switch or a specific VLAN.
-

## 34.47 show ip igmp snooping blocked-router

<b>Command Objective</b>	This command displays the blocked router ports for all VLANs or a specific VLAN, for a given switch or for all the switches (if no switch is specified).
<b>Syntax</b>	<code>show ip igmp snooping blocked-router [Vlan &lt;vlan-id/vfi-id&gt;]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>vlan &lt;vlan-id/vfi-id&gt;</b> - Displays the blocked router ports for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.</li></ul></li></ul> <p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p> <p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p> <p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<p><b>Single Instance</b></p> <pre>SEFOS# show ip igmp snooping blocked-router Vlan  Ports ----  - 1     Ex0/1, Ex0/2, Ex0/3, Ex0/4 2     Ex0/6, Ex0/7, Ex0/8</pre> <p><b>Multiple Instance</b></p> <pre>SEFOS# show ip igmp snooping blocked-router</pre>

---

Switch default

Vlan Ports

----

1 Ex0/1

Switch cust

Vlan Ports

----

1 Ex0/3

---

**Related Command(s)**

- **ip igmp snooping blocked-router** – Statically configures the blocked router ports for a VLAN.
-

## 34.48 show ip igmp snooping multicast-receivers

---

<b>Command Objective</b>	This command displays IGMP multicast host information for for all VLANs, a specific VLAN, or specific VLAN and group address, for a given switch or for all switches (if no switch is specified).
<b>Syntax</b>	<code>show ip igmp snooping multicast-receivers [Vlan &lt;vlan-id/vfi-id&gt; [Group &lt;Address&gt;]]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>vlan &lt;vlan-id/vfi-id&gt;</b> - Displays the displays IGMP multicast host information for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.</li></ul><hr/><p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p><p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p><p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p><hr/></li><li>• <b>Group</b> - Displays IGMP multicast host information for the multicast group address.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Note:</b>	<ul style="list-style-type: none"><li>• IGMP snooping must be enabled in the switch.</li><li>• The port leave mode for an interface must be set as exp-hosttrack.</li></ul>
<b>Example</b>	<b>Single Instance</b>  <code>SEFOS# show ip igmp snooping multicast-receivers</code>

---

---

Snooping Receiver Information

-----  
VLAN ID: 1 Group Address: 225.0.0.10

Receiver Port: Ex0/2

Attached Hosts: 12.0.0.10

Exclude Sources: None

VLAN ID: 1 Group Address: 225.0.0.20

Receiver Port: Ex0/2

Attached Hosts: 12.0.0.20

Include Sources: 14.0.0.10

Receiver Port: Ex0/4

Attached Hosts: 12.0.0.40

Include Sources: 14.0.0.20

**Multiple instance**

**SEFOS# show ip igmp snooping multicast-receivers**

Snooping Receiver Information

-----  
Switch switch1

VLAN ID: 1 Group Address: 225.0.0.20

Receiver Port: Ex0/4

Attached Hosts: 12.0.0.30

Include Sources: 14.0.0.10

Attached Hosts: 12.0.0.40

Exclude Sources: None

Switch switch2

VLAN ID: 1 Group Address: 225.0.0.20

Receiver Port: Ex0/2

Attached Hosts: 12.0.0.10

Exclude Sources: None

Attached Hosts: 12.0.0.20

Include Sources: 14.0.0.10

---

**Related Command(s)**

- **ip igmp snooping** - Enables IGMP snooping in the switch or a specific VLAN.
  - **ip igmp snooping leavemode exp-hosttrack** – Processes the leave messages using the explicit host tracking mechanism.
-



## 34.49 show ip igmp snooping port-cfg

<b>Command Objective</b>	This command displays IGS port configuration information for all Inner VLANs, a specific Inner VLAN ID, or a given switch.
<b>Syntax</b>	<pre>show ip igmp snooping port-cfg [{interface &lt;interface- type&gt; &lt;interface-id&gt; [InnerVlanId vlan-id(1-4094)]   switch &lt;switch_name&gt;}]</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>interface&lt;interface-type&gt; &lt;interface-id&gt;</b> - Displays IGS port configuration information for the interface type and interface identifier. The details to be provided are:<ul style="list-style-type: none"><li>▪ <b>&lt;interface-type&gt;</b> - Sets the type of interface. The interface can be:<ul style="list-style-type: none"><li>▪ <b>fastethernet</b> – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.</li><li>▪ <b>XL-ethernet</b> – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.</li><li>▪ <b>extreme-ethernet</b> – A version of Ethernet that supports data transfer up to 10 Gigabits per second.</li><li>▪ <b>i-lan</b> – Internal LAN created on a bridge per IEEE 802.1ap.</li></ul></li><li>▪ <b>&lt;interface-id&gt;</b> - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan. Only i-lan ID is provided, for interface type i-lan.</li></ul></li><li>• <b>InnerVlanId vlan-id(1-4094)</b> - Displays the IGS port configuration information for the Inner VLAN identifier. This value ranges from 1 to 4094.</li><li>• <b>switch &lt;switch_name&gt;</b> - Displays the IGS port configuration information for the specified context. This value represents unique name of the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<pre>Single Instance  SEFOS# show ip igmp snooping port-cfg Snooping Port Configurations ----- Snooping Port Configuration for Port 2</pre>

---

```
Leave Process mode is Normal Leave
Rate limit on the interface is 100
Max limit Type is Groups
Max limit is 20
Current member count is 0
Profile Id is 0
Snooping Port Configuration for Port 3
Leave Process mode is Fast Leave
Rate limit on the interface is -1
Max limit Type is Channels
Max limit is 500
Current member count is 0
Profile Id is 0
```

```
SEFOS# show ip igmp snooping port-cfg interface extreme-
ethernet 0/2
```

```
Snooping Port Configurations
-----
```

```
Snooping Port Configuration for Port 2
Leave Process mode is Normal Leave
Rate limit on the interface is 100
Max limit Type is Groups
Max limit is 20
Current member count is 0
Profile Id is 0
```

### **Multiple Instance**

```
SEFOS# show ip igmp snooping port-cfg
```

```
Snooping Port Configurations
-----
```

```
Snooping Port Configuration for Port 3
Leave Process mode is Fast Leave
Rate limit on the interface is 1000
Max limit Type is None
Max limit is 0
Current member count is 0
Profile Id is 0
Snooping Port Configuration for Port 4
```

---

---

```
Leave Process mode is Normal Leave
Rate limit on the interface is -1
Max limit Type is None
Max limit is 0
Current member count is 0
Profile Id is 1
Snooping Port Configuration for Port 6 and Inner Vlan Id 5
Leave Process mode is Normal Leave
Rate limit on the interface is 200
Max limit Type is None
Max limit is 0
Current member count is 0
Profile Id is 0
Snooping Port Configuration for Port 7 and Inner Vlan Id 0
Leave Process mode is Normal Leave
Rate limit on the interface is -1
Max limit Type is Channels
Max limit is 200
Current member count is 0
Profile Id is 1
Snooping Port Configuration for Port 7 and Inner Vlan Id 6
Leave Process mode is Normal Leave
Rate limit on the interface is -1
Max limit Type is Groups
Max limit is 100
Current member count is 0
Profile Id is 0

SEFOS# show ip igmp snooping port-cfg interface extreme-
ethernet 0/7

Snooping Port Configurations
-----

Switch switch1
Snooping Port Configuration for Port 7 and Inner Vlan Id 0
Leave Process mode is Normal Leave
Rate limit on the interface is -1
Max limit Type is Channels
Max limit is 200
```

---

```

-----
Current member count is 0
Profile Id is 1
Snooping Port Configuration for Port 7 and Inner Vlan Id 6
Leave Process mode is Normal Leave
Rate limit on the interface is -1
Max limit Type is Groups
Max limit is 100
Current member count is 0
Profile Id is 0

SEFOS# show ip igmp snooping port-cfg switch default
Snooping Port Configurations
-----
Switch default
Snooping Port Configuration for Port 3
Leave Process mode is Fast Leave
Rate limit on the interface is 1000
Max limit Type is None
Max limit is 0
Current member count is 0
Profile Id is 0
Snooping Port Configuration for Port 4
Leave Process mode is Normal Leave
Rate limit on the interface is -1
Max limit Type is None
Max limit is 0
Current member count is 0
Profile Id is 1
-----

```

**Related Command(s)**

- **ip igmp snooping leavemode** – Configures the port leave mode for an interface.
- **ip igmp snooping ratelimit** – Configures the rate limit for a downstream interface in units of the number of IGMP packets per second.
- **ip igmp snooping limit** – Configures the maximum limit type for an interface.
- **ip igmp snooping filter-profileId** – Configures the multicast profile index for a downstream interface.

## 34.50 show ip igmp snooping multicast-vlan

---

<b>Command Objective</b>	This command displays multicast VLAN statistics in a switch and displays various profiles mapped to the multicast VLANs.
--------------------------	--

---

<b>Syntax</b>	<code>show ip igmp snooping multicast-vlan</code>
---------------	---

---

<b>Mode</b>	Privileged EXEC Mode
-------------	----------------------

---

<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
----------------	---

---

<b>Example</b>	<p><b>Single Instance</b></p> <pre>SEFOS# show ip igmp snooping multicast-vlan Multicast VLAN Statistics ===== ----- Multicast VLAN disabled Profile ID -- Multicast VLAN ----- -- -----           1      --          1           2      --          2 -----</pre> <p><b>Multiple Instance</b></p> <pre>SEFOS# show ip igmp snooping multicast-vlan Multicast VLAN Statistics ===== ----- Multicast VLAN disabled Profile ID -- Multicast VLAN ----- -- -----           1      --          1 -----</pre> <pre>Switch cust Multicast VLAN disabled Profile ID -- Multicast VLAN ----- -- -----</pre>
----------------	---

---

---

1            --            1

---

**Related Command(s)**

- **ip igmp snooping multicast-vlan** – Enables or disables the multicast VLAN feature.
  - **mvr** - Enables the multicast VLAN feature. This command is applicable only for the code using industry standard commands.
-

## 34.51 ip igmp snooping clear counters

<b>Command Objective</b>	This command clears the IGMP snooping statistics maintained for VLAN(s).
<b>Syntax</b>	<code>ip igmp snooping clear counters [Vlan &lt;vlan-id/vfi-id&gt;]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>Vlan &lt;vlan-id/vfi-id&gt;</b> - Clears the IGMP snooping statistics maintained for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.</li></ul></li></ul> <p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p> <p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p> <p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<code>SEFOS(config)# ip igmp snooping clear counters vlan 4094</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ip igmp snooping retry-count</code> - Sets the maximum number of group-specific queries sent by the switch.</li><li>• <code>ip igmp snooping startup-query-count</code> - Sets the maximum number of general query messages sent out on switch startup, when the switch is configured as a querier.</li></ul>

## 34.52 ip igmp snooping send-query

---

<b>Command Objective</b>	This command configures the IGMP general query transmission feature upon the topology change in the switch.
<b>Syntax</b>	<code>ip igmp snooping send-query { enable   disable }</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>enable</b> - Enables the snooping query transmission status which generates IGMP query messages.</li><li>• <b>disable</b> - Disables the snooping query transmission status which stops the switch from generating IGMP query messages.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<code>SEFOS(config)# ip igmp snooping send-query enable</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp snooping globals</code> - Displays IGMP snooping information for all or specified VLAN(s).</li></ul>

---



## 34.53 ip igmp snooping static-group

<b>Command Objective</b>	<p>This command configures IGMP snooping static multicast in the multicast switch.</p> <p>This no form of the command removes the IGMP snooping static multicast in the multicast switch.</p>
<b>Syntax</b>	<pre>ip igmp snooping static-group &lt;mcast_addr&gt; ports &lt;ifXtype&gt; &lt;iface_list&gt;  no ip igmp snooping static-group &lt;mcast_addr&gt;</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>&lt;mcast_addr&gt;</b> - Configures the multicast address. This value ranges from 225.0.0.0. to 239.255.255.255.</li><li>• <b>&lt;ifXtype&gt;</b> - Configures snooping static multicast for the specified type of interface. The interface can be:<ul style="list-style-type: none"><li>▪ <b>fastethernet</b> – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.</li><li>▪ <b>XL-ethernet</b> – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.</li><li>▪ <b>extreme-ethernet</b> – A version of Ethernet that supports data transfer up to 10 Gigabits per second.</li><li>▪ <b>internal-lan</b> – Internal LAN created on a bridge per IEEE 802.1ap.</li><li>▪ <b>port-channel</b> – Logical interface that represents an aggregator which contains several ports aggregated together.</li></ul></li><li>• <b>&lt;iface list&gt;</b> - Configures snooping static multicast for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided, for interface types internal-lan and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3.</li></ul>
<b>Mode</b>	Config-VLAN Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<pre>SEFOS (config-vlan)# ip igmp snooping static-group 225.3.2.2 ports extreme-ethernet 0/2</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>snooping multicast-forwarding-mode</b>- Specifies the snooping multicast forwarding mode.</li><li>• <b>show ip igmp snooping forwarding-database static -</b></li></ul>

---

Displays static forwarding entries.

- **show ip igmp snooping groups static**— Displays IGMP group information.
-

## 34.54 ip igmp filter

---

**Command Objective** This command creates a multicast filter profile index for an interface. This value ranges from 1 to 4294967295.

The no form of the command deletes the multicast filter profile.

This command is a standardized implementation of the existing command `ip igmp snooping filter-profileId`. Its operation is similar to the existing command.

---

**Syntax** `ip igmp filter < profile number >`

`no ip igmp filter`

---

**Mode** Interface Configuration Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Example** `SEFOS(config-if)# ip igmp filter 1`

---

## 34.55 ip igmp max-groups

---

**Command Objective** This command configures the maximum number of multicast groups that can be learned on the interface. This value ranges from 0 to 254.

The no form of the command deletes the maximum number of multicast group configured for the interface.

This command is a standardized implementation of the existing command `ip igmp snooping limit`. Its operation is similar to the existing command.

---

**Syntax** `ip igmp max-groups <integer32>`

`no ip igmp max-groups`

---

**Mode** Interface Configuration Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Example** `SEFOS(config-if)# ip igmp max-groups 5`

---

## CHAPTER 35

# MLD Snooping

---

MLD (Multicast Listener Discovery) is a protocol used by IPv6 router to discover the presence of multicast listeners (that is, nodes willing to receive multicast packets) on its direct links, and to discover, specifically, which multicast address is of interest to those neighboring nodes. It is used by applications to listen to some multicast group.

Oracle MLDS software is designed in accordance with the FSAP (Flexible Software Architecture for Portability) frame to ensure a high level of portability.

- The list of CLI commands for the configuration of MLDS is common to both **Single Instance** and **Multiple Instance** except for a difference in the prompt that appears for the Switch with Multiple Instance support.

The prompt for the Global Configuration Mode is,

```
SEFOS (config) #
```

## 35.1 ipv6 mld snooping

---

<b>Command Objective</b>	<p>This command enables MLD snooping in the switch or a specific VLAN.</p> <p>Memory resources required by the MLDS module are allocated and the module starts running. It initializes semaphore creation, timer task RBTtree, hash table, and RBT Tree nodes. MLD snooping is enabled and disabled globally in all the existing VLAN interfaces.</p> <p>The no form of this command disables MLD snooping in the switch or a specific VLAN.</p>
<b>Syntax</b>	<pre>ipv6 mld snooping</pre> <pre>no ipv6 mld snooping</pre>
<b>Mode</b>	Global Configuration Mode/Config-VLAN Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	MLD snooping is globally disabled.
	<p><u>Note:</u></p> <ul style="list-style-type: none"><li>• GMRP has to be disabled for the MLDS to be enabled.</li><li>• The MLDS can be enabled for a VLAN, only if the MLDS is started in the switch and the VLAN is activated.</li></ul>
<b>Example</b>	<pre>SEFOS(config)# ipv6 mld snooping</pre> <pre>SEFOS(config-vlan)# ipv6 mld snooping</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set gmrp disabled</code> – Globally disables GMRP feature on all ports of a switch.</li><li>• <code>vlan active</code> - Activates a VLAN in the switch.</li><li>• <code>no shutdown snooping</code>- Starts the snooping in the switch.</li><li>• <code>show ipv6 mld snooping globals</code> – Displays the global MLD snooping information.</li><li>• <code>show ipv6 mld snooping</code> - Displays MLD snooping information for all VLANs or a specific VLAN.</li><li>• <code>snooping multicast-forwarding-mode</code>– Specifies the snooping multicast forwarding mode.</li></ul>

---

## 35.2 ipv6 mld snooping proxy-reporting

---

<b>Command Objective</b>	<p>This command enables proxy-reporting in the MLD snooping switch.</p> <p>Configuring proxy-reporting summarizes the report sent by downstream hosts. It is used to build internal membership states and reduces MLD network traffic. When a query is received, it generates reports as consolidated bitmaps in the table and forwards it to the routers based on the available host information.</p> <p>The no form of this command disables proxy-reporting in the MLD snooping switch.</p>
<b>Syntax</b>	<pre>ipv6 mld snooping proxy-reporting</pre> <pre>no ipv6 mld snooping proxy-reporting</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	Proxy-reporting is enabled.
	<p><u>Note:</u> Proxy-reporting can be enabled in the MLD snooping switch only if the proxy is disabled in the switch.</p>
<b>Example</b>	<pre>SEFOS(config)# ipv6 mld snooping proxy-reporting</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ip igmp proxy-service</code> - Enables IGMP proxy service functionality in the system and starts protocol operations.</li><li>• <code>show ipv6 mld snooping globals</code> – Displays the global MLD snooping information.</li></ul>

---

## 35.3 ipv6 mld snooping mrouter-time-out

---

<b>Command Objective</b>	<p>This command sets the MLD snooping router purge time-out after which the port gets deleted if no MLD router control packets are received. If the router control packet is received before the timer expiry, the timer is restarted.</p> <p>The no form of this command sets the MLD snooping router port purge time to default value. The value range for the time out is 60-600 seconds.</p>
<b>Syntax</b>	<pre>ipv6 mld snooping mrouter-time-out &lt;(60-600) seconds&gt;</pre> <pre>no ipv6 mld snooping mrouter-time-out</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	125 seconds
<b>Example</b>	<pre>SEFOS(config)# ipv6 mld snooping mrouter-time-out 75</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ipv6 mld snooping globals</code> – Displays the global MLD snooping information.</li></ul>

---



## 35.4 ipv6 mld snooping port-purge-interval

---

**Command Objective** This command sets the MLD snooping port purge time interval after which the port gets deleted if MLD reports are not received. This value ranges from 130 to 1225.

For each port on which report has been received, this timer runs for the configured time. This timer is restarted whenever a report message is received from a host on the specific port. If the timer expires, then, the learned port entry is purged from the multicast group.

The no form of this command sets the MLD snooping port purge time interval to default value.

---

**Syntax** `ipv6 mld snooping port-purge-interval <(130-1225) seconds>`  
`no ipv6 mld snooping port-purge-interval`

---

**Mode** Global Configuration Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Default** 260 seconds

---

**Example** `SEFOS(config)# ipv6 mld snooping port-purge-interval 200`

---

**Related Command(s)**

- `show ipv6 mld snooping globals` – Displays the MLD snooping information for all VLANs or a specific VLAN.
- `show ipv6 mld snooping` - Displays MLD snooping information for all VLANs or a specific VLAN.

---

## 35.5 ipv6 mld snooping report-suppression-interval

---

<b>Command Objective</b>	<p>This command sets the MLD snooping report-suppression interval for which MLDv1 report messages do not get forwarded onto the router ports for the same group.</p> <p>This value range is between 1 and 25. This timer is used when both proxy and proxy-reporting are disabled. This timer is started as soon as a report message for that group is forwarded out. Within this interval, if another report for the same group arrives, it will not be forwarded.</p> <p>The no form of this command sets the MLD snooping report-suppression interval to its default value.</p>
<b>Syntax</b>	<pre>ipv6 mld snooping report-suppression-interval &lt;(1-25) seconds&gt;  no ipv6 mld snooping report-suppression-interval</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	5 seconds
	<p><u>Note:</u> This time interval is used when both proxy and proxy-reporting are disabled.</p>
<b>Example</b>	<pre>SEFOS(config)# ipv6 mld snooping report-suppression- interval 20</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ipv6 mld snooping globals</code> – Displays the global MLD snooping information.</li></ul>

---

## 35.6 ipv6 mld snooping retry-count

---

<b>Command Objective</b>	<p>This command sets the maximum number of group-specific queries sent on a port on the reception of MLDv1 leave message.</p> <p>This value ranges from 1 to 5. When the switch receives leave message on a port, it sends group-specific query to check if there are any interested receivers in the group. The Retry Count defines the maximum number of queries sent by the switch before deleting the port from the group membership information in the forwarding database. If the query count exceeds the limit, the port is deleted and the leave message is forwarded to the routers.</p> <p>The no form of this command sets the maximum number of group-specific queries sent on a port, on the reception of leave message, to its default value.</p>
<b>Syntax</b>	<pre>ipv6 mld snooping retry-count &lt;1-5&gt;</pre> <pre>no ipv6 mld snooping retry-count</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	2
<b>Example</b>	<pre>SEFOS(config)# ipv6 mld snooping retry-count 3</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ipv6 mld snooping clear counters</code> - Clears the MLD snooping statistics maintained for VLAN(s).</li><li>• <code>show ipv6 mld snooping globals</code> – Displays the global MLD snooping information.</li></ul>

---

## 35.7 ipv6 mld snooping group-query-interval

---

<b>Command Objective</b>	<p>This command configures the time interval after which the switch sends a group-specific query on a port. This value ranges from 2 to 5.</p> <p>The no form of this command sets the group-specific query interval time to its default value.</p>
<b>Syntax</b>	<pre>ipv6 mld snooping group-query-interval &lt;(2-5) seconds&gt;</pre> <pre>no ipv6 mld snooping group-query-interval</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	2 seconds
<b>Example</b>	<pre>SEFOS(config)# ipv6 mld snooping group-query-interval 3</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ipv6 mld snooping globals</code> – Displays the global MLD snooping information.</li></ul>

---

## 35.8 ipv6 mld snooping report-forward

---

<b>Command Objective</b>	<p>This command configures the time interval after which the switch sends a group-specific query on a port, VLAN member ports, or router ports.</p> <p>The no form of this command sets the MLD report-forwarding status to default value. This configuration is not valid in proxy or proxy-reporting mode.</p>
<b>Syntax</b>	<pre>ipv6 mld snooping report-forward {all-ports   router-ports}  no ipv6 mld snooping report-forward</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>all-ports</b> - Configures the MLD reports to be forwarded on all the ports of a VLAN.</li><li>• <b>router-ports</b> - Configures the MLD reports to be forwarded only on router ports of a VLAN.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	router-ports
<b>Example</b>	<pre>SEFOS(config)# ipv6 mld snooping report-forward all-ports</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>show ipv6 mld snooping globals</b> – Displays the global MLD snooping information.</li></ul>

---

## 35.9 ipv6 mld snooping version

---

<b>Command Objective</b>	This command configures the operating version of the MLD snooping switch for a specific VLAN.
<b>Syntax</b>	<code>ipv6 mld snooping version {v1   v2}</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>v1</b> - Configures the version as MLDv1. MLDS report is accessed only with group address. It is provided with leave request option.</li><li>• <b>v2</b> - Configures the version as MLDv2. MLDS report is accessed with source and group address.</li></ul>
<b>Mode</b>	Config-VLAN Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	v2
	<u>Note:</u> The configuration can be done only for the VLANs that are activated in the switch.
<b>Example</b>	<code>SEFOS(config-vlan)#ipv6 mld snooping version v1</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>vlan active</b>- Activates a VLAN in the switch.</li><li>• <b>show ipv6 mld snooping</b> – Displays MLD snooping information for all VLANs or a specific VLAN.</li></ul>

---

## 35.10 ipv6 mld snooping fast-leave

---

**Command Objective** This command enables fast leave processing for a specific VLAN. When fast leave is disabled, on reception of a leave message, the switch checks if there are any interested receivers for the group by sending a group-specific query before removing the port from the forwarding table. If fast leave is enabled, the switch does not send a group-specific query and immediately removes the port from the forwarding table.

The no form of the command disables fast leave processing for a specific VLAN.

---

**Syntax** `ipv6 mld snooping fast-leave`  
`no ipv6 mld snooping fast-leave`

---

**Mode** Config-VLAN Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Default** Disabled

---

Note: The configuration can be done only for the VLANs that are activated in the switch.

---

**Example** `SEFOS(config-vlan)# ipv6 mld snooping fast-leave`

---

**Related Command(s)**

- `vlan active` - Activates a VLAN in the switch.
- `show ipv6 mld snooping` - Displays MLD snooping information for all VLANs or a specific VLAN.

---

## 35.11 ipv6 mld snooping querier

---

<b>Command Objective</b>	<p>This command configures the MLD snooping switch as a querier for a specific VLAN. The switch starts sending general queries at regular time intervals. When the router port gets operationally down and there are no router ports in the switch, the switch continues the querier functionality.</p> <p>The no form of this command configures the MLD snooping switch as non-querier for a specific VLAN.</p>
<b>Syntax</b>	<pre>ipv6 mld snooping querier</pre> <pre>no ipv6 mld snooping querier</pre>
<b>Mode</b>	Config-VLAN Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	Non-querier
	<p><u>Note:</u> The configuration can be done only for the VLANs that are activated in the switch.</p>
<b>Example</b>	<pre>SEFOS(config-vlan)# ipv6 mld snooping querier</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>vlan active</code> - Activates a VLAN in the switch.</li><li>• <code>show ipv6 mld snooping</code> – Displays MLD snooping information for all VLANs or a specific VLAN.</li></ul>

---



## 35.12 ipv6 mld snooping query-interval

---

**Command Objective** This command sets the time period for which the switch waits after sending a group-specific query to determine if the hosts are still interested in a specific multicast group. This value ranges from 60 to 600. In proxy-reporting mode, general queries are sent on all downstream interfaces with this interval, only if the switch is the querier.

The no form of this command sets the MLDS query interval to default value.

---

**Syntax** `ipv6 mld snooping query-interval <(60 - 600) seconds>`  
`no ipv6 mld snooping query-interval`

---

**Mode** Config-VLAN Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Default** 125 seconds

---

Note: The configuration can be done only for the VLANs that are activated in the switch.

---

**Example** `SEFOS(config-vlan)# ipv6 mld snooping query-interval 65`

---

**Related Command(s)**

- `vlan active` - Activates a VLAN in the switch.
- `show ipv6 mld snooping` – Displays MLD snooping information for all VLANs or a specific VLAN.

---

## 35.13 ipv6 mld snooping mrouter

---

**Command Objective** This command configures statically the router ports for a VLAN.

The no form of this command deletes the statically configured router ports for a VLAN. By default the router port list is set to none.

---

**Syntax**

```
ipv6 mld snooping mrouter <interface-type> <0/a-b, 0/c, ...>
```

```
no ipv6 mld snooping mrouter <interface-type> <0/a-b, 0/c, ...>
```

---

**Parameter Description**

- **<interface-type>**- Statically configures the router ports for the specified type of interface. The interface can be:
  - **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
  - **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gigabits per second.
  - **internal-lan** – Internal LAN created on a bridge per IEEE 802.1ap.
  - **port-channel** – Logical interface that represents an aggregator which contains several ports aggregated together.
- **<0/a-b, 0/c, ...>**- Configures, statically, the router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided, for interface types internal-lan and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3.

---

**Mode** Config-VLAN Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

Note:

- The configuration can be done only for the VLANs that are activated in the switch.
  - The specified interface can be set as router ports for the VLAN, only if the interfaces are configured as member ports for that VLAN.
- 

**Example** `SEFOS(config-vlan)# ipv6 mld snooping mrouter extreme-ethernet 0/1-3`

---

---

**Related Command(s)**

- `vlan active` - Activates a VLAN in the switch.
  - `ports` - Statically configures a VLAN entry with the required member ports, untagged ports or forbidden ports, and activates the VLAN..
  - `show ipv6 mld snooping mrouter` - Displays the router ports for all the VLANs or a specific VLAN.
-

## 35.14 debug ipv6 mld snooping

---

<b>Command Objective</b>	<p>This command enables tracing and generates debug statements for the specified debug options in MLD snooping module.</p> <p>The no form of the command disables debugging for the specified options in MLD snooping module.</p>
<b>Syntax</b>	<pre>debug ipv6 mld snooping ([init] [resources] [tmr] [src] [grp] [qry] [vlan] [pkt] [fwd] [mgmt]) [switch &lt;switch_name&gt;]  no debug ipv6 mld snooping ([init] [resources] [tmr] [src] [grp] [qry] [vlan] [pkt] [fwd] [mgmt]) [switch &lt;switch_name&gt;]</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>init</b> - Generates Init and Shutdown trace messages at the instances when the module is initiated or shut down. The information is logged in a file.</li><li>• <b>resources</b> - Generates System Resources management trace messages when there is a change in the resource status. The information is logged in a file.</li><li>• <b>tmr</b> - Generates Timer trace messages at the instances where timers are involved. The information is logged in a file.</li><li>• <b>src</b> - Generates trace messages when source information is involved.</li><li>• <b>grp</b> - Generates trace messages when group information is involved.</li><li>• <b>qry</b> - Generates trace messages for query-related events.</li><li>• <b>vlan</b> - Generates trace messages when VLAN-related information is involved.</li><li>• <b>pkt</b> - Generates packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets.</li><li>• <b>fwd</b> - Generates trace messages when forwarding database is involved.</li><li>• <b>mgmt</b> - Generates debug statements for management plane functionality traces.</li><li>• <b>switch</b> - Generates trace messages for the specified switch context. This value is a string of size 32.</li></ul>
<b>Mode</b>	Privileged EXEC Mode

---

---

<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	Debugging is disabled.
<u>Note:</u>	The debug statements are displayed only if MLDS is started in the switch.
<b>Example</b>	<pre>SEFOS# debug ipv6 mld snooping init resources mgmt pkt vlan src tnr switch default</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ipv6 mld snooping</code> - Enables MLD snooping in the switch or a specific VLAN.</li><li>• <code>show debugging</code> - Displays state of each debugging option.</li></ul>

---

## 35.15 show ipv6 mld snooping mrouter

---

<b>Command Objective</b>	This command displays the router ports for all the VLANs or a specific VLAN. Interface, ports (type of ports), and switch details are displayed.
<b>Syntax</b>	<code>show ipv6 mld snooping mrouter [Vlan &lt;vlan-id/vfi-id&gt;] [detail]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>vlan &lt;vlan-id/vfi-id&gt;</b> - Displays the router ports for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.<hr/><p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p><p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p><p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p><hr/></li></ul></li><li>• <b>detail</b> - Displays detailed information about the router ports.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<p><b>Single Instance</b></p> <pre>SEFOS# show ipv6 mld snooping mrouter Vlan 1 Vlan   Ports -----   1     Ex0/1(static)</pre> <p><b>Multiple Instance</b></p>

---

---

```
SEFOS# show ipv6 mld snooping mrouter
```

```
Switch cust1
```

```
Vlan    Ports
```

```
-----
```

```
      2 Ex0/4 (static)
```

```
Switch cust2
```

```
Vlan    Ports
```

```
-----
```

```
      1 Ex0/10 (static)
```

```
      2 Ex0/9 (dynamic)
```

---

**Related Command(s)**

- **ipv6 mld snooping mrouter** – Statically configures the router ports for a VLAN.
-

## 35.16 show ipv6 mld snooping globals

---

<b>Command Objective</b>	This command displays the global MLD snooping information for all VLANs or a specific VLAN. Information such as MLD snooping globally enabled, MLD snooping operationally enabled, Transmit Query on topology change and so on.
<b>Syntax</b>	<b>show ipv6 mld snooping globals</b>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<b>Single Instance</b>  <pre>SEFOS# show ipv6 mld snooping globals Snooping Configuration ----- MLD Snooping globally enabled MLD Snooping is operationally enabled Transmit Query on Topology Change  globally disabled Multicast forwarding mode is MAC based Proxy globally disabled Proxy reporting globally enabled Filter is disabled Router port purge interval is 125 seconds Port purge interval is 260 seconds Report forward interval is 5 seconds Group specific query interval is 2 seconds Reports are forwarded on router ports Queries are forwarded on non-router ports Group specific query retry count is 2 Multicast VLAN disabled Leave config level is Vlan based Report processing config level is on non-router ports</pre> <b>Multiple Instance</b>  <pre>SEFOS# show ipv6 mld snooping globals Switch default</pre>

---



---

## Snooping Configuration

---

-----  
MLD Snooping globally enabled  
MLD Snooping is operationally enabled  
Multicast forwarding mode is MAC based  
Proxy globally disabled  
Proxy reporting globally enabled  
Filter is disabled  
Router port purge interval is 125 seconds  
Port purge interval is 260 seconds  
Report forward interval is 5 seconds  
Group specific query interval is 2 seconds  
Reports are forwarded on router ports  
Queries are forwarded on non-router ports  
Group specific query retry count is 2  
Multicast VLAN disabled  
Leave config level is Vlan based  
Report processing config level is on non-router ports

---

### Related Command(s)

- **ipv6 mld snooping** - Enables MLD snooping in the switch.
  - **ipv6 mld snooping proxy-reporting** - Enables proxy-reporting in the MLD snooping switch.
  - **snooping multicast-forwarding-mode** - Specifies the snooping multicast forwarding mode.
  - **ipv6 mld snooping mrouter-time-out** - Sets the MLD snooping router purge time-out after which the port gets deleted if no MLD router control packets are received.
  - **ipv6 mld snooping port-purge-interval** - Sets the MLD snooping port purge time interval after which the port gets deleted if MLD reports are not received.
  - **ipv6 mld snooping report-suppression-interval** - Sets the MLD snooping report-suppression time interval.
  - **ipv6 mld snooping retry-count** - Sets the maximum number of group-specific queries sent on a port on the reception of MLDv1 done message.
  - **ipv6 mld snooping group-query-interval** - Configures the time interval that the switch waits for the membership reports from the interested receivers, for the given multicast group, after sending out query messages.
-

- 
- **ipv6 mld snooping report-forward** - Specifies whether the MLD reports are forwarded on all VLAN member ports or router ports.
-

## 35.17 show ipv6 mld snooping

<b>Command Objective</b>	This command displays MLD snooping information for all VLANs or a specific VLAN. Information such as MLD snooping enabled, MLD configured version is v2, and so on.
<b>Syntax</b>	<code>show ipv6 mld snooping [Vlan &lt;vlan-id/vfi-id&gt;]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>vlan &lt;vlan-id/vfi-id&gt;</b> - Displays MLD snooping information for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.</li></ul></li></ul> <p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p> <p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p> <p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<b>Single Instance</b> <pre>SEFOS# show ipv6 mld snooping Vlan 1 Snooping VLAN Configuration for the VLAN 1   MLD Snooping enabled   MLD configured version is V2   Fast leave is disabled   Snooping switch is configured as Querier   Snooping switch is acting as Non-Querier</pre>

---

Startup Query Count is 2  
Startup Query Interval is 31 seconds  
Query interval is 125 seconds  
Other Querier Present Interval is 255 seconds  
Port Purge Interval is 157 seconds  
Max Response Code is 10000, Time is 10 seconds

### Multiple Instance

#### SEFOS# show ipv6 mld snooping

Switch default  
Snooping VLAN Configuration for the VLAN 1  
MLD Snooping enabled  
MLD configured version is V2  
Fast leave is disabled  
Snooping switch is configured as Querier  
Snooping switch is acting as Non-Querier  
Startup Query Count is 2  
Startup Query Interval is 31 seconds  
Query interval is 125 seconds  
Other Querier Present Interval is 255 seconds  
Port Purge Interval is 260 seconds  
Max Response Code is 10000, Time is 10 seconds

---

#### Related Command(s)

- **ipv6 mld snooping** - Enables MLD snooping in the switch.
  - **ipv6 mld snooping port-purge-interval** - Sets the MLD snooping port purge time interval after which the port gets deleted if MLD reports are not received.
  - **ipv6 mld snooping version** - Sets the operating version of the MLD snooping switch for a specific VLAN.
  - **ipv6 mld snooping fast-leave** - Enables fast leave processing for a specific VLAN.
  - **ipv6 mld snooping querier** - Configures the MLD snooping switch as a querier for a specific VLAN.
  - **ipv6 mld snooping query-interval** - Sets the time period with which the general queries are sent by the MLD snooping switch when it is configured as a querier on the VLAN.
  - **ip igmp snooping max-response-code** - Sets the maximum response code sent in general queries.
-



## 35.18 show ipv6 mld snooping groups

<b>Command Objective</b>	This command displays the MLDS group information for all VLANs, a specific VLAN, or a specific VLAN and group address. Information displayed in the output is Snooping Group information, VLAN ID, group address, filter mode and so on.
<b>Syntax</b>	<pre>show ipv6 mld snooping groups [Vlan &lt;vlan-id/vfi-id&gt; [Group &lt;Address&gt;]]</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>vlan &lt;vlan-id/vfi-id&gt;</b> - Displays MLD snooping group information for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.</li></ul><p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p><p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p><p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p></li><li>• <b>Group &lt;Address&gt;</b> - Group address of the VLAN ID.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<p><b>Single Instance</b></p> <pre>SEFOS# show ipv6 mld snooping groups Snooping Group information ----- VLAN ID:1  Group Address: ff07::1:1 Filter Mode: EXCLUDE</pre>

---

Exclude sources: None  
ASM Receiver Ports: Ex0/1

### Multiple Instance

**SEFOS# show ipv6 mld snooping groups**

Switch cust1

Snooping Group information

-----  
VLAN ID:2 Group Address: ff02::1:1

Filter Mode: EXCLUDE

Exclude sources: None

Receiver Ports:

Ex0/5

VLAN ID:2 Group Address: ff02::2:2

Filter Mode: EXCLUDE

Exclude sources: None

Receiver Ports:

Ex0/5

Switch cust2

Snooping Group information

-----  
VLAN ID:2 Group Address: ff02::1:1

Filter Mode: EXCLUDE

Exclude sources: None

Receiver Ports:

Ex0/10

VLAN ID:2 Group Address: ff02::2:2

Filter Mode: EXCLUDE

Exclude sources: None

Receiver Ports:

Ex0/11

---

### Related Command(s)

- **ipv6 mld snooping** - Enables MLD snooping in the switch.
-

## 35.19 show ipv6 mld snooping forwarding-database

---

**Command Objective** This command displays multicast forwarding entries for all VLANs or a specific VLAN. The information displayed is VLAN, source address, group address and ports.

---

**Syntax** `show ipv6 mld snooping forwarding-database [Vlan <vlan-id/vfi-id>]`

---

**Parameter Description**

- **vlan <vlan-id/vfi-id>** - Displays multicast forwarding entries for the specified VLAN / VFI ID. This value ranges from 1 to 65535.
  - **<vlan -id>** - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.
  - **<vfi-id>** - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.

---

**Note:** The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.

**Note:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.

**Note:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.

---

---

**Mode** Privileged EXEC Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Example** **Single Instance**

**/\* IP based \*/**

```
SEFOS# show ipv6 mld snooping forwarding-database
```

Vlan	Source Address	Group Address	Ports
1	fe80::7	ff07::1:1	Ex0/1

**/\* MAC based \*/**

---



---

**SEFOS# show ipv6 mld snooping forwarding-database**

Vlan	MAC-Address	Ports
1	33:33:00:01:00:01	Ex0/1

**Multiple Instance**

**SEFOS# show ipv6 mld snooping forwarding-database**

Switch cust1

Vlan	MAC-Address	Ports
2	33:33:00:01:00:01	Ex0/5
2	33:33:00:02:00:02	Ex0/5

Switch cust2

Vlan	MAC-Address	Ports
2	33:33:00:01:00:01	Ex0/9, Ex0/10
2	33:33:00:02:00:02	Ex0/9, Ex0/11

---

**Related Command(s)**

- **ipv6 mld snooping** - Enables MLD snooping in the switch.
-

## 35.20 show ipv6 mld snooping statistics

<b>Command Objective</b>	This command displays MLD snooping statistics for all VLANs or a specific VLAN. The information displayed is snooping statistics, general queries received, group specific queries received, group and source specific queries received and so on.
<b>Syntax</b>	<code>show ipv6 mld snooping statistics [Vlan &lt;vlan-id/vfi-id&gt;]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>vlan &lt;vlan-id/vfi-id&gt;</b> - Displays MLD snooping statistics for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.</li></ul></li></ul> <p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p> <p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p> <p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<b>Single Instance</b>  <pre>SEFOS# show ipv6 mld snooping statistics Snooping Statistics for VLAN 1   General queries received : 0   Group specific queries received : 0   Group and source specific queries received : 0   ASM reports received : 1   SSM reports received : 0</pre>

---

```
IS_INCLUDE messages received : 0
IS_EXCLUDE messages received : 0
TO_INCLUDE messages received : 0
TO_EXCLUDE messages received : 0
ALLOW messages received : 0
Block messages received : 0
Done messages received : 0
General queries transmitted : 0
Group specific queries transmitted : 0
Group and source specific queries transmitted : 0
ASM reports transmitted : 0
SSM reports transmitted : 0
Done messages transmitted : 0
Unsuccessful joins recieved count Per Vlan : 0
Active/Successful joins recieved count Per Vlan: 0
Active Groups count: 0
Packets dropped : 0
```

### **Multiple Instance**

#### **SEFOS# show ipv6 mld snooping statistics**

```
Switch cust1
Snooping Statistics for VLAN 2
  General queries received : 0
  Group specific queries received : 0
Group and source specific queries received : 0
ASM reports received : 0
SSM reports received : 3
IS_INCLUDE messages received : 0
IS_EXCLUDE messages received : 0
TO_INCLUDE messages received : 0
TO_EXCLUDE messages received : 0
ALLOW messages received : 0
Block messages received : 0
Done messages received : 0
General queries transmitted : 2
Group specific queries transmitted : 0
ASM reports transmitted : 0
```

---

---

```
SSM reports transmitted : 0
Done messages transmitted : 0
Packets dropped : 0
Switch cust2
Snooping Statistics for VLAN 2
  General queries received : 2
  Group specific queries received : 0
Group and source specific queries received : 0
ASM reports received : 58
SSM reports received : 0
IS_INCLUDE messages received : 0
IS_EXCLUDE messages received : 0
TO_INCLUDE messages received : 0
TO_EXCLUDE messages received : 0
ALLOW messages received : 0
Block messages received : 0
Done messages received : 0
General queries transmitted : 0
Group specific queries transmitted : 0
ASM reports transmitted : 0
SSM reports transmitted : 3
Done messages transmitted : 0
Packets dropped : 0
```

---

**Related Command(s)**

- **ipv6 mld snooping** - Enables MLD snooping in the switch.
-

## 35.21 ipv6 mld snooping clear counters

<b>Command Objective</b>	This command clears the MLD snooping statistics maintained for VLAN(s).
<b>Syntax</b>	<code>ipv6 mld snooping clear counters [Vlan &lt;vlanid/vfi_id&gt;]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>Vlan &lt;vlan-id/vfi-id&gt;</b> - Clears MLD snooping statistics for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.</li></ul></li></ul> <p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p> <p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p> <p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<code>SEFOS(config)# ipv6 mld snooping clear counters vlan 150</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ipv6 mld snooping retry-count</code> - Sets the maximum number of group-specific queries sent by the switch.</li></ul>

## 35.22 debug ipv6 mld snooping all

---

**Command Objective** This command enables tracing and generates debug statements for all levels in MLD snooping module.

The no form disables debugging for all levels in MLD snooping module.

---

**Syntax**

```
debug ipv6 mld snooping all
```

```
no debug ipv6 mld snooping all
```

---

**Mode** Privileged EXEC Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Default** Debugging is disabled.

---

Note: The debug statements are displayed only if MLDS is started in the switch.

---

**Example** SEFOS# debug ipv6 mld snooping all switch default

---

**Related Command(s)**

- `ipv6 mld snooping` - Enables MLD snooping in the switch or a specific VLAN.
- `show debugging` - Displays state of each debugging option.

---

## CHAPTER 36

# IGMP

---

**Oracle IGMP (Internet Group Management Protocol)** is a portable implementation of the Internet Group Management Protocol Version 3. It implements the IGMP router functionalities required by the Multicast Routing Protocol.

Oracle IGMP conforms to RFC 3376 for IGMP v3 router functionality. Oracle IGMP supports the MIB defined in draft-ietf-magma-rfc2933-update-00.txt.

The deployment of the Oracle IGMP router can be within a routing domain that uses any Multicast Routing Protocol. Oracle IGMP informs MRPs about group membership messages and leave messages.

## 36.1 set ip igmp

---

<b>Command Objective</b>	This command enables or disables IGMP globally or on a particular interface.
<b>Syntax</b>	<code>set ip igmp {enable disable}</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>enable</b> - Enables IGMP feature globally or on a particular interface.</li><li>• <b>disable</b> - Disables IGMP feature globally or on a particular interface. This removes all dynamic multicast entries, stops all the timers for route entries, and disables IGMP on all the IGMP-enabled interfaces.</li></ul>
<b>Mode</b>	Global Configuration Mode / Interface Configuration Mode (VLAN/Router Port)
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	disable
<b>Example</b>	<pre>SEFOS(config)# set ip igmp enable SEFOS(config-if)# set ip igmp enable</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ip igmp proxy-service / ip igmp proxy service</code> - Enables IGMP Proxy service in the system.</li><li>• <code>ip igmp limit</code> - Configures global group limit for IGMP.</li><li>• <code>ip igmp explicit-tracking</code> - Enables explicit channel tracking on IGMPv3 interface.</li><li>• <code>ip igmp list - except Group-list Id</code> - Configures the IGMP grouplist for an interface.</li><li>• <code>show ip igmp global-config</code> - Displays the global configuration of IGMP.</li></ul>

---



## 36.2 ip igmp immediate-leave

---

<b>Command Objective</b>	<p>This command enables immediate leave processing on the interface by intimating the Multicast Routing Protocol on the last member leaving the group. This must be enabled only on those interfaces where there is single host. This feature can also be enabled on those interfaces having more than one host, provided all the hosts are v3 hosts in V3 mode.</p> <p>The no form of the command disables immediate leave processing on the interface.</p>
<b>Syntax</b>	<pre>ip igmp immediate-leave  no ip igmp immediate-leave</pre>
<b>Mode</b>	Interface Configuration Mode (VLAN/Router Port)
<b>Package</b>	Enterprise and Metro_
<b>Default</b>	Immediate leave processing is disabled.
<b>Example</b>	<pre>SEFOS(config-if)# ip igmp immediate-leave</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp interface</code> - Displays the interface configuration of IGMP.</li></ul>

---

## 36.3 ip igmp version

---

<b>Command Objective</b>	<p>This command configures the IGMP version on the interface. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN.</p> <p>The no form of the command sets the default IGMP version on the interface.</p>
<b>Syntax</b>	<pre>ip igmp version { 1   2   3 }  no ip igmp version</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• 1 - Configures the IGMP version 1.</li><li>• 2 - Configures the IGMP version 2.</li><li>• 3 - Configures the IGMP version 3.</li></ul>
<b>Mode</b>	Interface Configuration Mode (VLAN/Router Port)
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	version 2
<b>Example</b>	<pre>SEFOS(config-if)# ip igmp version 3</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp interface</code> - Displays the interface configuration of IGMP.</li><li>• <code>ip igmp explicit-tracking</code> - Enables explicit channel tracking on IGMPv3 interface.</li></ul>

---

## 36.4 ip igmp query-interval

---

**Command Objective** This command configures the frequency at which IGMP host-query packets are transmitted on the interface. This value ranges from 1 to 65535.

The no form of the command resets the IGMP query-interval to its default value.

---

**Syntax** `ip igmp query-interval <value (1-65535) seconds>`  
`no ip igmp query-interval`

---

**Mode** Interface Configuration Mode (VLAN/Router Port)

---

**Package** Enterprise and Metro\_E

---

**Default** 125 seconds

---

Note:

- Query interval should be greater than 10 for IGMP Version 2 and 3.
- Query interval configuration is not allowed for IGMP Version 1.

---

**Example** `SEFOS(config-if)# ip igmp query-interval 30`

---

**Related Command(s)**

- `set ip igmp` - Enables or disables IGMP.
- `ip igmp version` - Sets the IGMP version on the interface.
- `ip igmp query-interval` - Configures the IGMP query interval for the interface.
- `show ip igmp interface` - Displays the interface configuration of IGMP.

---

## 36.5 ip igmp query-max-response-time

---

<b>Command Objective</b>	This command configures the maximum IGMP query response value for the interface. This value ranges from 0 to 255.  The no form of the command resets the max query response to its default value.
<b>Syntax</b>	<pre>ip igmp query-max-response-time &lt;value (0-255) seconds&gt;  no ip igmp query-max-response-time</pre>
<b>Mode</b>	Interface Configuration Mode (VLAN/Router Port)
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	100 seconds
	<u>Note:</u> This command executes only if query interval is greater than one-tenth of Max Response Time.
<b>Example</b>	<pre>SEFOS(config-if)# ip igmp query-max-response-time 20</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ip igmp query-interval</code> - Configures the IGMP query interval for the interface.</li><li>• <code>show ip igmp interface</code> - Displays the interface configuration of IGMP.</li><li>• <code>show ip igmp groups</code> - Displays the IGMP groups' information.</li></ul>

---

## 36.6 ip igmp robustness

---

<b>Command Objective</b>	<p>This command configures the IGMP robustness value for the interface. This value ranges from 1 to 255.</p> <p>The robustness variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the robustness value may be increased.</p> <p>The no form of the command resets the robustness value to its default value.</p>
<b>Syntax</b>	<pre>ip igmp robustness &lt;value(1-255)&gt;</pre> <pre>no ip igmp robustness</pre>
<b>Mode</b>	Interface Configuration Mode (VLAN/Router Port)
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	2
<b>Example</b>	<pre>SEFOS(config-if)# ip igmp robustness 100</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp interface</code> - Displays the interface configuration of IGMP.</li></ul>

---

## 36.7 ip igmp last-member-query-interval

---

**Command Objective** This command configures the IGMP last member query interval for the interface. The last member query interval is the maximum response time inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. This value is tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This value ranges from 0 to 255.

The no form of the command sets the last member query interval to its default value.

---

**Syntax** `ip igmp last-member-query-interval <value(0-255)>`  
`no ip igmp last-member-query-interval`

---

**Mode** Interface Configuration Mode (VLAN/Router Port)

---

**Package** Enterprise and Metro\_E

---

**Default** 10

---

Note: This command executes only if the IGMP version on this interface is set to 2 or 3.

---

**Example** `SEFOS(config-if)# ip igmp last-member-query-interval 100`

---

**Related Command(s)**

- `set ip igmp` - Enables or disables IGMP.
- `ip igmp version` - Sets the IGMP version on the interface.
- `ip igmp immediate-leave` - Enables immediate leave processing on the interface.
- `show ip igmp interface` - Displays the interface configuration of IGMP.

---

## 36.8 ip igmp static-group

---

<b>Command Objective</b>	<p>This command adds the static group membership on the interface.</p> <p>The no form of the command deletes the static group membership on the interface.</p>
<b>Syntax</b>	<pre>ip igmp static-group &lt;Group Address&gt; [source &lt;Source Address&gt;]  no ip igmp static-group &lt;Group Address&gt; [source &lt;Source Address&gt;]</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>&lt;Group Address&gt;</b> - Configures the group IP address as a static group member on the interface.</li><li>• <b>source&lt;Source Address&gt;</b> - Configures the source IP address of a system where multicast data packets originate.</li></ul>
<b>Mode</b>	Interface Configuration Mode (VLAN/Router Port)
<b>Package</b>	Enterprise and Metro_E
<b>Example</b>	<pre>SEFOS(config-if)# ip igmp static-group 224.1.2.3 source 12.0.0.1</pre>
<b>Note:</b>	The IGMP version on the interface must be set to 3 for configuring static group along with source information.
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>set ip igmp</b> - Enables or disables IGMP.</li><li>• <b>ip igmp version</b> - Sets the IGMP version on the interface.</li><li>• <b>show ip igmp groups</b> - Displays the IGMP groups' information.</li><li>• <b>show ip igmp sources</b> - Displays the IGMP sources information.</li><li>• <b>show ip igmp interface</b> - Displays the interface configuration of IGMP.</li></ul>

---

## 36.9 no ip igmp

---

<b>Command Objective</b>	<p>This command deletes the IGMP capable interface. That is, it disables IGMP feature in a particular interface.</p> <p>At least one of the interface configuration commands must have been executed to create the IGMP interface.</p>
<b>Syntax</b>	<code>no ip igmp</code>
<b>Mode</b>	Interface Configuration Mode (VLAN/Router Port)
<b>Package</b>	Enterprise and Metro_E
<b>Example</b>	<code>SEFOS(config-if)# no ip igmp</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp interface</code> - Displays the interface configuration of IGMP.</li></ul>

---



## 36.10 debug ip igmp

---

<b>Command Objective</b>	<p>This command enables the tracing of the IGMP module as per the configured debug levels. The trace statements are generated for the configured trace levels.</p> <p>The no form of the command disables the tracing of IGMP module as per the configured debug levels. The trace statements are not generated for the configured trace levels.</p>
<b>Syntax</b>	<pre>debug ip igmp ( [i/o][grp][qry][tmr][mgmt] [all] ) no debug ip igmp ( [i/o][grp][qry][tmr][mgmt] [all] )</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>i/o</b> - Generates debug statements for input or output traces.</li><li>• <b>grp</b> - Generates debug statements for group-related traces.</li><li>• <b>qry</b> - Generates debug statements for query-related traces.</li><li>• <b>tmr</b> - Generates debug statements for timer-related traces.</li><li>• <b>mgmt</b> - Generates debug statements for management configuration traces.</li><li>• <b>all</b> - Generates debug statements for all kinds of traces.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	Tracing of the IGMP module is disabled.
<b>Example</b>	<pre>SEFOS# debug ip igmp all</pre>

---

## 36.11 show ip igmp global-config

---

<b>Command Objective</b>	This command displays the global configuration of IGMP.
<b>Syntax</b>	<code>show ip igmp global-config</code>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Example</b>	<pre>SEFOS# show ip igmp global-config IGMP is globally enabled IGMP Proxy is globally disabled in the system IGMP Global State Limit : 0 out of max 10</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip igmp</code> - Enables or disables IGMP.</li><li>• <code>ip igmp proxy-service / ip igmp proxy service</code> - Enables IGMP Proxy service in the system.</li><li>• <code>ip igmp limit</code> - Configures global group limit for IGMP.</li></ul>

---

## 36.12 show ip igmp interface

---

**Command Objective** This command displays the interface configuration of IGMP.

---

**Syntax** `show ip igmp interface [{ Vlan <vlan-id> | <vlan-id/vfi-id> <interface-id> | <IP-interface-type> <IP-interface-number> }]`

---

**Parameter Description**

- **Vlan <vlan-id/vfi-id>** - Displays IGMP Interface configuration for the specified VLAN / VFI ID. This value ranges from 1 to 65535.
  - **<vlan -id>** - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.
  - **<vfi-id>** - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.

---

Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.

Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.

Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.

---

- **<interface-type>** - Displays the IGMP interface configuration for the specified type of interface. The interface can be:
    - **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
    - **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gigabits per second.
    - **i-lan** – Internal LAN created on a bridge per IEEE 802.1ap.
  - **<interface-id>** - Displays IGMP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1.
-

---

Only i-lan and port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.

- **<IP-interface-type>** - Displays IGMP interface configuration for the specified L3 pseudowire interface in the system.
- **<IP-interface-number>** - Displays IGMP interface configuration for the specified L3 pseudowire interface identifier. This is a unique value that represents the specific interface. This value ranges from 1 to 65535 for pseudowire interface.

---

Note: Maximum number of pseudowire interfaces supported in the system is 100.

---

---

**Mode** Privileged EXEC Mode

---

**Package** Enterprise and Metro\_E

---

**Example**

**SEFOS# show ip igmp interface**

```
IGMP is globally disabled
vlan1, line protocol is down
  Internet Address is 12.0.0.7/8
  IGMP is disabled on interface
  Current IGMP router version is 2
  IGMP Interface State Limit 0 out of max 10
  IGMP Exempt GroupList Id 100
  IGMP query interval is 125 seconds
  Last member query response interval is 10 seconds
  IGMP max query response time is 100 seconds
  Robustness value is 2
  IGMP querying router is 0.0.0.0
  Fast leave is disabled on this interface
  Number of multicast groups joined 1

Slot0/3, line protocol is down
  Internet Address is 0.0.0.0/0
  IGMP is disabled on interface
  Current IGMP router version is 3
  Explicit Tracking is enabled
  IGMP Interface State Limit 0 out of max 2
  IGMP query interval is 125 seconds
  Last member query response interval is 10 seconds
  IGMP max query response time is 100 seconds
```

---

---

```
Robustness value is 2
IGMP querying router is 0.0.0.0 (this system)
Fast leave is disabled on this interface
No multicast groups joined
```

---

**Related Command(s)**

- **set ip igmp** - Enables or disables IGMP.
  - **ip igmp immediate-leave** - Enables immediate leave processing on the interface.
  - **ip igmp version** - Sets the IGMP version on the interface.
  - **ip igmp query-interval** - Sets the IGMP query interval for the interface.
  - **ip igmp query-max-response-time** - Sets the IGMP max query response value for the interface.
  - **ip igmp robustness** - Sets the IGMP robustness value for the interface.
  - **ip igmp last-member-query-interval** - Sets the IGMP last member query interval for the interface.
  - **ip igmp static-group** - Adds the static group membership on the interface.
  - **no ip igmp** - Deletes the IGMP capable interface.
  - **ip igmp list - except Group-list Id** - Configures the IGMP grouplist for an interface.
  - **ip igmp explicit-tracking** - Enables explicit channel tracking on IGMPv3 interface.
-

## 36.13 show ip igmp groups

---

<b>Command Objective</b>	This command displays the IGMP group information.
<b>Syntax</b>	<code>show ip igmp groups</code>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Example</b>	<pre>SEFOS# show ip igmp groups I - Include Mode,   E - Exclude Mode S - Static Mbr,    D - Dynamic Mbr GroupAddress  Flg Iface   UpTime   ExpiryTime LastReporter ----- 224.5.5.5     S   vlan2   [0d 00:00:22.28] [0d 00:00:00.00] 20.0.0.1 226.7.7.7    IS  vlan3   [0d 00:00:04.59] [0d 00:00:00.00] 30.0.0.1</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ip igmp static-group</code> - Adds the static group membership on the interface.</li><li>• <code>ip igmp version</code> - Sets the IGMP version on the interface.</li></ul>

---

## 36.14 show ip igmp sources

---

<b>Command Objective</b>	This command displays the IGMP source information.
<b>Syntax</b>	<code>show ip igmp sources</code>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Example</b>	<pre>SEFOS# show ip igmp sources I - Include Mode, E - Exclude Mode S - Static Mbr, D - Dynamic Mbr F - Forward List, N - Non-Forward List GroupAddress  Iface  SrcAddress  Flg  ExpiryTime LastReporter ----- --- 226.7.7.7      vlan3  12.0.0.1   ISF  [0d 00:00:00.00] 30.0.0.1</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ip igmp static-group</code> - Adds the static group membership on the interface.</li><li>• <code>ip igmp version</code> - Sets the IGMP version on the interface.</li></ul>

---

## 36.15 show ip igmp statistics

---

**Command Objective** This command displays the IGMP statistics information.

---

**Syntax**

```
show ip igmp statistics [{ Vlan <vlan-id/vfi-id> |  
<interface-type> <interface-id> | <IP-interface-type> <IP-  
interface-number>}]
```

---

**Parameter Description**

- **Vlan <vlan-id/vfi-id>** - Displays IGMP statistics information for the specified VLAN / VFI ID. This value ranges from 1 to 65535.
  - **<vlan -id>** - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.
  - **<vfi-id>** - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.

---

Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.

Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.

Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.

---

- **<interface-type>** - Displays IGMP statistics information for the specified type of interface. The interface can be:
    - **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
    - **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gigabits per second.
    - **i-lan** – Internal LAN created on a bridge per IEEE 802.1ap.
  - **<interface-id>** - Displays the IGMP statistics information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port
-



---

number is 1. Only i-lan and port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.

- **<IP-interface-type>** - Displays IGMP statistics information for the specified L3 pseudowire interface in the system.
- **<IP-interface-number>** - Displays IGMP statistics information for the specified L3 pseudowire interface identifier. This is a unique value that represents the specific interface . This value ranges from 1 to 65535 for pseudowire interface.

---

Note: Maximum number of pseudowire interfaces supported in the system is 100.

---

---

**Mode** Privileged EXEC Mode

---

**Package** Enterprise and Metro\_E

---

**Example** **SEFOS# show ip igmp statistics**

```
IGMP Statistics for vlan1
  Number of General queries received 1
  Number of Group Specific queries received 0
  Number of Group and Source Specific queries received 0
  Number of v1/v2 reports received 0
  Number of v3 reports received 8
  Number of v2 leaves received 0
  Number of General queries transmitted 1
  Number of Group Specific queries transmitted 1
  Number of Group and Source Specific queries transmitted
2
IGMP Statistics for vlan3
  Number of General queries received 0
  Number of Group Specific queries received 0
  Number of Group and Source Specific queries received 0
  Number of v1/v2 reports received 0
  Number of v3 reports received 6
  Number of v2 leaves received 0
  Number of General queries transmitted 1
  Number of Group Specific queries transmitted 0
  Number of Group and Source Specific queries transmitted
0
```

---

**Related Command(s)**

- **ip igmp static-group** - Adds the static group membership on the interface.

---

- 
- `ip igmp version` - Sets the IGMP version on the interface.
-

## 36.16 show provider-bridge tunnel-mac-address

---

<b>Command Objective</b>	This command displays the tunnel MAC address configured for the layer 2 protocols in the given switch.
<b>Syntax</b>	<code>show provider-bridge tunnel-mac-address [switch &lt;context_name&gt;]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li><code>switch &lt;context_name&gt;</code> - Displays the tunnel MAC address configured for layer 2 protocols for the specified context. This represents a unique name for the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Example</b>	<pre>SEFOS# show provider-bridge tunnel-mac-address Switch default VLAN tunnel MAC address ----- Dot1x tunnel MAC address : 01:00:0c:cd:cd:d3 LACP tunnel MAC address  : 01:00:0c:cd:cd:d4 STP tunnel MAC address   : 01:00:0c:cd:cd:d0 MVRP tunnel MAC address  : 01:00:0c:cd:cd:d5 MMRP tunnel MAC address  : 01:00:0c:cd:cd:d6 GVRP tunnel MAC address  : 01:00:0c:cd:cd:d1 GMRP tunnel MAC address  : 01:00:0c:cd:cd:d2</pre>

---

## 36.17 ip igmp limit

---

<b>Command Objective</b>	<p>This command configures global group limit for IGMP. This value is the total number of multicast groups allowed globally. This value ranges from 1 to 255.</p> <p>The no form of the command deletes the global group limit for IGMP. This takes the default value of zero.</p>
<b>Syntax</b>	<pre>ip igmp limit &lt;integer(1-255)&gt;  no ip igmp limit</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Note:</b>	This command executes only if IGMP is enabled globally.
<b>Example</b>	<pre>SEFOS(config)# ip igmp limit 25</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip igmp</code> - Enables or disables IGMP.</li><li>• <code>show ip igmp global-config</code> - Displays the global configuration of IGMP.</li></ul>

---

## 36.18 ip igmp group-list

---

<b>Command Objective</b>	This command configures the IGMP group list.  The no form of the command deletes configured IGMP group list.
<b>Syntax</b>	<pre>ip igmp group-list &lt;integer&gt; &lt;ip-address&gt; &lt;mask&gt;  no ip igmp group-list &lt;integer&gt; [&lt;ip-address&gt; &lt;mask&gt;]</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• &lt;integer&gt; - Configures the group list identifier. This value ranges from 1 to 4294967295.</li><li>• &lt;ip-address&gt; - Configures the multicast IP address of the group.</li><li>• &lt;mask&gt; - Configures the subnet mask of the IGMP group.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Example</b>	<pre>SEFOS(config)# ip igmp group-list 100 235.0.0.1 255.255.255.255</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip igmp group-list</code> - Displays all global group lists of IGMP.</li></ul>

---

## 36.19 ip igmp limit - except group list id

---

<b>Command Objective</b>	This command configures the IGMP grouplist for an interface.  The no form of the command deletes the configured IGMP group list on the interface. This takes the default value of zero.
<b>Syntax</b>	<pre>ip igmp limit &lt;integer(1-255)&gt; [except &lt;Group-List id&gt;]  no ip igmp limit</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>&lt;integer (1-255)&gt;</b> - Configures the interface limit. This indicates the total number of multicast groups that can be allowed for this interface. This value ranges from 1 to 255.</li><li>• <b>except &lt;Group-List id&gt;</b> - Configures the exception group identifier for the interface. This group list will be exempted from limiting on this interface. This value ranges from 1 to 4294967295.</li></ul>
<b>Mode</b>	Interface Configuration Mode (Router / VLAN)
<b>Package</b>	Enterprise and Metro_E
<b>Note:</b>	This command executes only if IGMP is enabled on the interface.
<b>Example</b>	<pre>SEFOS (config-if)# ip igmp limit 2 except 10</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>set ip igmp</b> - Enables or disables IGMP on the interface.</li><li>• <b>show ip igmp interface</b> - Displays the interface configuration of IGMP.</li></ul>

---

## 36.20 show ip igmp group-list

---

**Command Objective** This command displays all the global group list of IGMP.

---

**Syntax** `show ip igmp group-list`

---

**Mode** Privileged EXEC Mode

---

**Package** Enterprise and Metro\_E

---

**Example** `SEFOS# show ip igmp group-list`

```
GroupList : 11
Group Address : 225.0.0.0 Mask : 255.0.0.0
Group Address : 226.0.0.0 Mask : 255.0.0.0
GroupList : 12
-----
Group Address : 228.0.0.0 Mask : 255.0.0.0
```

---

**Related Command(s)**

- `ip igmp group-list` - Configures the IGMP grouplist.

---

## 36.21 ip igmp explicit-tracking

---

**Command Objective** This command enables explicit channel tracking on IGMPv3 interface. Channel tracking is the ability of a system to keep track of each individual host that is joined to a particular multicast group or channel.

The no form of the command disables explicit channel tracking on IGMPv3 interface.

---

**Syntax** `ip igmp explicit-tracking`  
`no ip igmp explicit-tracking`

---

**Mode** Interface Configuration Mode (VLAN/Router Port)

---

**Package** Enterprise and Metro\_E

---

**Default** Channel tracking is disabled.

---

Note:

- This configuration is effective only if IGMP is enabled on the interface.
- Explicit tracking can be enabled for IGMP version 3 interface.

---

**Example** `SEFOS(config-if)# ip igmp explicit-tracking`

---

**Related Command(s)**

- `set ip igmp` - Enables or disables IGMP on the interface.
- `ip igmp version` - Sets the IGMP version on the interface.
- `show ip igmp interface` - Displays the interface configuration of IGMP.
- `show ip igmp membership` - Displays the IGMP membership information.

---



## 36.22 show ip igmp membership

<b>Command Objective</b>	This command displays the membership information for groups or channels.
<b>Syntax</b>	<code>show ip igmp membership [[&lt;mcast_addr&gt;] {[tracked]   [all]}]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>&lt;mcast addr&gt;</code> - Displays membership information for multicast groups.</li><li>• <code>all</code> - Displays the membership information all multicast groups.</li><li>• <code>tracked</code> - Displays the membership information for the multicast groups for which channel tracking is enabled.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Note:</b>	<ul style="list-style-type: none"><li>• This command displays the output only if IGMP is enabled globally.</li><li>• This command is similar to the CISCO command but the output display is limited compared to the CISCO output display.</li></ul>
<b>Example</b>	<pre>SEFOS# show ip igmp membership 239.255.255.254 IGMP is globally enabled  Flags: A - Aggregate T - tracked S - Static , R - Reported through v3 1,2,3 - The version of IGMP  Channel/Group-Flags: / - Filtering entry (Exclude mode (S,G),Include mode (G))  Reporter: &lt;mac-or-ip-address&gt; - last reporter if group isnot explicitly tracked &lt;n&gt;/&lt;m&gt; - &lt;n&gt; reporter in include mode,&lt;m&gt; reporter in exclude  Channel/Group          Flags Interface Reporter -----</pre>

---

```
* ,239.255.255.254      2AS   vlan2      0.0.0.0
```

---

**Related Command(s)**

- **set ip igmp** - Enables or disables IGMP.
  - **ip igmp explicit-tracking** - Enables explicit channel tracking on IGMPv3 interface.
-

## **CHAPTER 37**

# **IGMP Proxy**

---

IGMP Proxy (Internet Group Management Protocol Proxy) implementation is used to learn and proxy group membership information, and then forward multicast packets based on the learned membership information. The IGMP Proxy learns membership information from IGMP hosts in downstream interfaces (interface to which hosts are connected) and substitutes (proxy) the information to upstream interfaces (interface to which upstream router is connected), based on the requirements of IGMP hosts.

IGMP Proxy is used mainly in edge devices. It reduces the cost of the devices, as well as the operational overhead because it does not need to support more complicated multicast routing protocols such as Protocol Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP).

## 37.1 ip igmp proxy-service

---

<b>Command Objective</b>	<p>This command enables IGMP Proxy service functionality in the system and starts protocol operations.</p> <p>The no form of the command disables IGMP Proxy service functionality in the system stops performing protocol operations.</p>
<b>Syntax</b>	<pre>ip igmp proxy-service</pre> <pre>no ip igmp proxy-service</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	IGMP proxy service is disabled.
	<p><u>Note:</u> This command executes only if the IGMP module is enabled globally and PIM and DVMRP modules are disabled in the switch.</p>
<b>Example</b>	<pre>SEFOS(config)# ip igmp proxy-service</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip igmp</code> - Enables or disables IGMP globally or on a particular interface.</li><li>• <code>set ip dvmrp</code> - Enables or disables DVMRP in the switch.</li><li>• <code>set ip pim</code> - Enables or disables PIM.</li><li>• <code>ip multicast</code> - Enables PIM globally.</li><li>• <code>show ip igmp-proxy mrouter</code> - Displays the upstream interface configuration of IGMP Proxy.</li></ul>

---

## 37.2 ip igmp proxy service

---

<b>Command Objective</b>	<p>This command enables IGMP Proxy service functionality in the system.</p> <p>This command is a standardized implementation of the existing command <code>ip igmp proxy-service</code>. Its operation is similar to the existing command. This feature has been included to adhere to the Industry Standard CLI syntax.</p>
<b>Syntax</b>	<code>ip igmp proxy service</code>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	IGMP proxy service is disabled.
	<p><u>Note:</u> This command executes only if the IGMP module is enabled globally and also PIM and DVMRP modules are disabled in the switch.</p>
<b>Example</b>	<code>SEFOS(config)# ip igmp proxy service</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip igmp</code> - Enables or disables IGMP globally or on a particular interface.</li><li>• <code>set ip dvmrp</code> - Enables or disables DVMRP in the switch.</li><li>• <code>set ip pim</code> - Enables or disables PIM.</li><li>• <code>show ip igmp-proxy mrouter</code> - Displays the upstream interface configuration of IGMP Proxy.</li></ul>

---

## 37.3 ip igmp-proxy mrouter

---

<b>Command Objective</b>	<p>This command configures the interface as an upstream multicast router interface.</p> <p>The no form of the command removes the interface from the upstream multicast router interface list.</p>
<b>Syntax</b>	<pre>ip igmp-proxy mrouter</pre> <pre>no ip igmp-proxy mrouter</pre>
<b>Mode</b>	Interface Configuration Mode (VLAN/Router Port)
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Note:</b>	<p>This command executes only if,</p> <ul style="list-style-type: none"><li>• IGMP is enabled on the interface.</li><li>• IGMP Proxy is enabled in the system.</li></ul>
<b>Example</b>	<pre>SEFOS(config-if)# ip igmp-proxy mrouter</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip igmp</code> - Enables or disables IGMP on a particular interface.</li><li>• <code>ip igmp proxy-service / ip igmp proxy service</code> - Enables IGMP proxy service functionality in the system.</li><li>• <code>show ip igmp-proxy mrouter</code> - Displays the upstream interface configuration of IGMP Proxy.</li></ul>

---

## 37.4 ip igmp mroute proxy

---

<b>Command Objective</b>	<p>This command configures the interface as an upstream interface.</p> <p>This command is a standardized implementation of the existing command <code>ip igmp-proxy mrouter</code>. Its operation is similar to the existing command. This feature has been included to adhere to the Industry Standard CLI syntax.</p>
<b>Syntax</b>	<code>ip igmp mroute proxy</code>
<b>Mode</b>	Interface Configuration Mode (VLAN/Router Port)
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Note:</b>	<p>This command executes only if,</p> <ul style="list-style-type: none"><li>• IGMP is enabled on the interface.</li><li>• IGMP Proxy is enabled in the system.</li></ul>
<b>Example</b>	<code>SEFOS(config-if)# ip igmp mroute proxy</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip igmp</code> - Enables or disables IGMP globally or on a particular interface.</li><li>• <code>ip igmp proxy-service / ip igmp proxy service</code> - Enables IGMP proxy service functionality in the system.</li><li>• <code>show ip igmp-proxy mrouter</code> - Displays the upstream interface configuration of IGMP Proxy.</li></ul>

---

## 37.5 ip igmp-proxy mrouter-time-out

---

<b>Command Objective</b>	This command configures the upstream interface purge interval, after which the IGMP version on upstream interface will switch back to the configured version. The purge interval ranges between 60 and 600 in seconds.
<b>Syntax</b>	<code>ip igmp-proxy mrouter-time-out &lt;(60 - 600) seconds&gt;</code>
<b>Mode</b>	Interface Configuration Mode (VLAN/Router Port)
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	Purge interval - 125 Seconds
<b>Note:</b>	This command executes only if IGMP Proxy is enabled in the system
<b>Example</b>	<code>SEFOS(config-if)# ip igmp-proxy mrouter-time-out 100</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ip igmp proxy-service / ip igmp proxy service</code> - Enables IGMP proxy service functionality in the system.</li><li>• <code>show ip igmp-proxy mrouter</code> - Displays the upstream interface configuration of IGMP Proxy.</li></ul>

---



## 37.6 ip igmp-proxy mrouter-version

---

<b>Command Objective</b>	This command configures the version of the IGMP Proxy device on the upstream interface. This should be configured based on the version of IGMP router present in the upstream interface. The configured version is set to the operating version of the IGMP interface when the router interface purge timer expires for the interface.
<b>Syntax</b>	<code>ip igmp-proxy mrouter-version { 1   2   3 }</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• 1 - Configures the IGMP Version 1.</li><li>• 2 - Configures the IGMP Version 2.</li><li>• 3 - Configures the IGMP Version 3.</li></ul>
<b>Mode</b>	Interface Configuration Mode (VLAN/Router Port)
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	3
	<u>Note:</u> This command executes only if IGMP Proxy is enabled in the system
<b>Example</b>	<code>SEFOS(config-if)# ip igmp-proxy mrouter-version 2</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ip igmp proxy-service / ip igmp proxy service</code> - Enables IGMP proxy service functionality in the system.</li><li>• <code>show ip igmp-proxy mrouter</code> - Displays the upstream interface configuration of IGMP Proxy.</li></ul>

---

## 37.7 show ip igmp-proxy mrouter

<b>Command Objective</b>	This command displays the upstream interface configuration of IGMP Proxy.
<b>Syntax</b>	<code>show ip igmp-proxy mrouter [Vlan &lt;vlan-id/vfi-id&gt;]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>Vlan &lt;vlan-id/vfi-id&gt;</b> - Displays upstream interface configuration of IGMP Proxy for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.</li></ul></li></ul> <p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p> <p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p> <p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Note:</b>	This command executes only if the IGMP Proxy module is enabled globally.
<b>Example</b>	<pre>SEFOS# show ip igmp-proxy mrouter IfName/IfId OperVersion CfgVersion UpTime/VersionExpiryTime PurgeIntvl ----- vlan3/35 IGMPv3 IGMPv3 [0d 00:08:01.31]/0 125 vlan4 /36 IGMPv2 IGMPv2 [0d 00:00:25.67]/0 100  SEFOS# show ip igmp-proxy mrouter vlan 4 IfName/IfId OperVersion CfgVersion</pre>

---

UpTime/Version	ExpiryTime	PurgeIntvl
vlan4	/36	IGMPv2
		IGMPv2
		[0d 00:00:48.40]/0
		100

---

**Related Command(s)**

- **ip igmp proxy-service / ip igmp proxy service** - Enables IGMP proxy service functionality in the system.
  - **ip igmp-proxy mrouter / ip igmp mroute proxy** - Configures the interface as an upstream interface.
  - **ip igmp-proxy mrouter-time-out** - Configures the upstream interface purge interval.
  - **ip igmp-proxy mrouter-version** - Configures the version of IGMP on upstream interface.
-

## 37.8 show ip igmp-proxy forwarding-database

<b>Command Objective</b>	This command displays the multicast forwarding information.
<b>Syntax</b>	<pre>show ip igmp-proxy forwarding-database [{Vlan &lt;vlan-id/vfi-id&gt;  group &lt;group-address&gt;   source &lt;source-address&gt;}]</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>vlan &lt;vlan-id/vfi-id&gt;</b> - Displays multicast forwarding information for the specified VLAN / VFI ID. This value ranges from 1 to 65535.<ul style="list-style-type: none"><li>▪ <b>&lt;vlan -id&gt;</b> - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.</li><li>▪ <b>&lt;vfi-id&gt;</b> - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.</li></ul><p>Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.</p><p>Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.</p><p>Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.</p></li><li>• <b>group&lt;group-address&gt;</b> - Displays the IP multicast group address for which multicast registrations are received.</li><li>• <b>source&lt;source-address&gt;</b> - Displays the unicast source IP address of the data source that sends multicast datagrams for the registered multicast groups.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Note:</b>	This command executes only if the IGMP Proxy module is enabled globally.
<b>Example</b>	<pre>SEFOS# show ip igmp-proxy forwarding-database IGMP Proxy Multicast Routing table</pre>

```

-----
(Source, Group), Uptime/Expires(seconds)
Incoming Interface: Interface
Outgoing Interface:
Interface, State
(13.0.0.10, 234.0.0.3) , [0d 00:23:55.65]/ 26
  Incoming Interface : vlan3
  Outgoing InterfaceList :
    vlan1, Forwarding
    vlan4, Forwarding
(13.0.0.10, 234.0.0.4) , [0d 00:23:55.65]/ 13
  Incoming Interface : vlan3
  Outgoing InterfaceList :
    vlan1, Forwarding
    vlan2, Forwarding
    vlan4, Forwarding
(13.0.0.11, 234.0.0.3) , [0d 00:23:55.65]/ 107
  Incoming Interface : vlan3
  Outgoing InterfaceList :
    vlan2, Forwarding
    vlan4, Forwarding

```

```

SEFOS# show ip igmp-proxy forwarding-database group
234.0.0.4

```

```

IGMP Proxy Multicast Routing table
-----

```

```

(Source, Group) , Uptime/Expires(seconds)
Incoming Interface: Interface
Outgoing Interface:
Interface, State
(13.0.0.10, 234.0.0.4) , [0d 00:24:30.29]/ 77
  Incoming Interface : vlan3
  Outgoing InterfaceList :
    vlan1, Forwarding
    vlan2, Forwarding
    vlan4, Forwarding

```

```

SEFOS# show ip igmp-proxy forwarding-database source
13.0.0.11

```

```

IGMP Proxy Multicast Routing table
-----

```

---

```
(Source, Group) , Uptime/Expires(seconds)
Incoming Interface: Interface
Outgoing Interface:
Interface, State
(13.0.0.11, 234.0.0.3) , [0d 00:24:49.36]/ 53
  Incoming Interface : vlan3
  Outgoing InterfaceList :
    vlan2, Forwarding
    vlan4, Forwarding
```

---

**Related Command(s)**

- **ip igmp proxy-service / ip igmp proxy service** - Enables IGMP proxy service functionality in the system.
  - **show ip igmp-proxy mrouter** - Displays the upstream interface configuration of IGMP Proxy.
-

## **CHAPTER 38**

# **PIM**

---

PIM (Protocol Independent Multicast) is a multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. Multicast IP routing protocols are used to distribute data to multiple recipients. Using multicast, a source can send a single copy of data to a single multicast address, which is then distributed to an entire group of recipients. A multicast group identifies a set of recipients that are interested in a particular data stream, and is represented by an IP address from a well-defined range. Data sent to this IP address is forwarded to all members of the multicast group.

PIM is independent of unicast routing protocol and can be operated in two modes: dense and sparse. It is designed to provide scalable inter-domain multicast routing across the Internet. PIM provides multicast routing and forwarding capability to the switch. It maintains the integrity of the hardware based multicast forwarding table with respect to the forwarding table existing in the software. It is independent of the underlying unicast routing protocol and uses the information from the Unicast Routing protocol.

## 38.1 set ip pim

<b>Command Objective</b>	This command globally enables or disables PIM feature in the switch.
<b>Syntax</b>	<code>set ip pim { enable   disable }</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>enable</code> - Enables PIM feature in the switch.</li><li>• <code>disable</code> - Disables PIM feature in the switch.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	Disable
	<u>Note:</u> IGMP proxy service must be disabled in the system, before enabling the PIM globally.
<b>Example</b>	<code>SEFOS (config)# set ip pim enable</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>no ip igmp proxy-service</code> - Disables IGMP proxy service in the system.</li><li>• <code>set ip pim graft-retry interval</code> - Configures the time before which graft is retransmitted upon no receipt of Graft ACK.</li><li>• <code>set ip pim lan-prune-delay</code> - Enables or disables the LanPruneDelay bit configured for the router interface to advertise the LAN delay.</li><li>• <code>ip pim lan-delay</code> - Configures the LanDelay configured for the router interface.</li><li>• <code>ip pim override-interval</code> - Configures the override interval configured for router interface.</li><li>• <code>ip pim dr-priority</code> - Configures the designated router priority value configured for the router interface.</li><li>• <code>ip pim componentId</code> - Adds the interface to the PIM component.</li><li>• <code>ip pim bsr-candidate - value / ip pim bsr-candidate - vlan</code> - Configures the local interface as a candidate Bootstrap Router.</li><li>• <code>ip pim message-interval</code> - Configures the frequency at which PIM Join or Prune messages are transmitted on the PIM interface.</li></ul>



- 
- **ip pim query-interval** - Configures the frequency at which PIM hello messages are transmitted on this interface.
  - **rp-static rp-address** - Configures the address of the interface, which will be advertised as a Static-RP.
  - **rp-candidate holdtime** - Configures the holdtime of the component when it is a candidate RP in the local domain.
  - **rp-candidate rp-address** - Configures the address of the interface, which will be advertised as a Candidate-RP.
  - **set mode** - Sets the component mode to sparse or dense.
  - **set ip pim source-active interval** - Configures the time duration for which the SRM control messages would be originated by the router after a data packet is received.
  - **ip pim state-refresh disable** - Disables the SRM processing and forwarding.
  - **set ip pim state-refresh origination-interval** - Configures the interval between successive SRM (State Refresh Messages) control messages originated and sent out by the router.
  - **set ip pim static-rp** - Enables or disables the static RP configuration status.
  - **ip pim component** - Configures the PIM component in the router and enters into PIM component mode.
  - **set ip pim pmbr** - Enables or disables the PIM Multicast Border Router (PMBR) Status.
  - **set ip pim regstop-ratelimit-period** - Configures the period over which RP monitors the number of register packets after sending the register stop message.
  - **set ip pim rp-switchperiod** - Configures the time period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree.
  - **set ip pim rp-threshold** - Configures the threshold at which the RP (Rendezvous Point) initiates switching to source specific shortest path tree.
  - **set ip pim spt-switchperiod** - Configures the time period (in seconds) over which the data rate is to be monitored for switching to shortest path tree.
  - **set ip pim threshold** - Configures the Shortest Path Tree (SPT) group or source threshold.
-

- 
- `show ip pim mroute` - Displays the PIM multicast information.
  - `show ip pim thresholds` - Displays the threshold configured for SPT, RP thresholds, and rate limit values for both SM.
  - `show ip pim component` - Displays the component information. The component ID value ranges between 1 and 255.
  - `show ip pim rp-static` - Displays the static RP information.
  - `show ip pim bsr` - Displays the BSR information.
  - `show ip pim rp-set` - Displays the RP-set information.
  - `show ip pim rp-candidate` - Displays the candidate RP information.
  - `show ip pim neighbor` - Displays the router's PIM neighbors' information.
  - `show ip pim interface` - Displays the router's PIM interfaces.
  - `debug ip pim` - Enables the tracing of the PIM module as per the configured debug levels.
  - `no ip pim interface` - Deletes an interface at PIM level.
  - `ip pim bidir-enable` - Enables the Bidirectional PIM feature.
  - `ip pim bidir-offer-interval` - Configures the Bidir-PIM offer interval in milliseconds.
  - `ip pim bidir-offer-limit` - Configures the Bidir-PIM offer limit.
  - `show ip pim rp-hash` - Displays the elected RP for the multicast group address with the mask length.
  - `show ip pim interface df` - Displays the df states of all the PIM interfaces.
-

## 38.2 ip multicast

---

<b>Command Objective</b>	This command globally enables PIM feature in the switch.  This command is a standardized implementation of the existing command <code>set ip pim</code> . Its operation is similar to the existing command.
<b>Syntax</b>	<code>ip multicast</code>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	PIM feature is disabled in the switch.
	<u>Note:</u> IGMP proxy service must be disabled in the system, before enabling the PIM globally.
<b>Example</b>	<code>SEFOS (config)# ip multicast</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>no ip igmp proxy-service</code> - Disables IGMP proxy service in the system.</li><li>• <code>set ip pim graft-retry interval</code> - Configures the time before which graft is retransmitted upon no receipt of Graft ACK.</li><li>• <code>set ip pim lan-prune-delay</code> - Enables or disables the LanPruneDelay bit configured for the router interface to advertise the LAN delay.</li><li>• <code>ip pim lan-delay</code> - Configures the LanDelay configured for the router interface.</li><li>• <code>ip pim override-interval</code> - Configures the override interval configured for router interface.</li><li>• <code>ip pim dr-priority</code> - Configures the designated router priority value configured for the router interface.</li><li>• <code>ip pim componentId</code> - Adds the interface to the PIM component.</li><li>• <code>ip pim bsr-candidate - value / ip pim bsr-candidate - vlan</code> - Configures the local interface as a candidate Bootstrap Router.</li><li>• <code>ip pim message-interval</code> - Configures the frequency at which PIM Join or Prune messages are transmitted on the PIM interface.</li></ul>

---

- 
- **ip pim query-interval** - Configures the frequency at which PIM hello messages are transmitted on this interface.
  - **rp-static rp-address** - Configures the address of the interface, which will be advertised as a Static-RP.
  - **rp-candidate holdtime** - Configures the holdtime of the component when it is a candidate RP in the local domain.
  - **rp-candidate rp-address** - Configures the address of the interface, which will be advertised as a Candidate-RP.
  - **set mode** - Sets the component mode to sparse or dense.
  - **set ip pim source-active interval** - Configures the time duration for which the SRM control messages would be originated by the router after a data packet is received.
  - **ip pim state-refresh disable** - Disables the SRM processing and forwarding.
  - **set ip pim state-refresh origination-interval** - Configures the interval between successive SRM (State Refresh Messages) control messages originated and sent out by the router.
  - **set ip pim static-rp** - Enables or disables the static RP configuration status.
  - **ip pim component** - Configures the PIM component in the router and enters into PIM component mode.
  - **set ip pim pmbr** - Enables or disables the PIM Multicast Border Router (PMBR) Status.
  - **set ip pim regstop-ratelimit-period** - Configures the period over which RP monitors the number of register packets after sending the register stop message.
  - **set ip pim rp-switchperiod** - Configures the time period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree.
  - **set ip pim rp-threshold** - Configures the threshold at which the RP (Rendezvous Point) initiates switching to source specific shortest path tree.
  - **set ip pim spt-switchperiod** - Configures the time period (in seconds) over which the data rate is to be monitored for switching to shortest path tree.
  - **set ip pim threshold** - Configures the Shortest Path Tree (SPT) group or source threshold.
-

- 
- `show ip pim mroute` - Displays the PIM multicast information.
  - `show ip pim thresholds` - Displays the threshold configured for SPT, RP thresholds, and rate limit values for both SM.
  - `show ip pim component` - Displays the component information. The component ID value ranges between 1 and 255.
  - `show ip pim rp-static` - Displays the static RP information.
  - `show ip pim bsr` - Displays the BSR information.
  - `show ip pim rp-set` - Displays the RP-set information.
  - `show ip pim rp-candidate` - Displays the candidate RP information.
  - `show ip pim neighbor` - Displays the router's PIM neighbors' information.
  - `show ip pim interface` - Displays the router's PIM interfaces.
  - `debug ip pim` - Enables the tracing of the PIM module as per the configured debug levels.
  - `no ip pim interface` - Deletes an interface at PIM level.
  - `ip pim bidir-enable` - Enables the Bidirectional PIM feature.
  - `ip pim bidir-offer-interval` - Configures the Bidir-PIM offer interval in milliseconds.
  - `ip pim bidir-offer-limit` - Configures the Bidir-PIM offer limit.
  - `show ip pim rp-hash` - Displays the elected RP for the multicast group address with the mask length.
  - `show ip pim interface df` - Displays the df states of all the PIM interfaces.
-

## 38.3 ip pim version

<b>Command Objective</b>	<p>This command configures version number of the PIM protocol in the switch.</p> <p>This command is a complete standardized implementation of the existing command. This feature has been included in adherence to the Industry Standard CLI syntax.</p>
<b>Syntax</b>	<pre>ip pim version { 1   2 }</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• 1 - Configures the version as PIM version 1. In PIMv1 , the range of supported multicast groups can be limited with an Access Control List (ACL).</li></ul> <hr/> <p>PIM version 1 is currently not supported.</p> <hr/> <ul style="list-style-type: none"><li>• 2 - Configures the version as PIM version 2. PIMv2 provides a standards-compliant equivalent to Auto-RP, called the bootstrap router method.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Default</b>	PIM Version - 2
<b>Package</b>	Enterprise and Metro_E
<b>Example</b>	<pre>SEFOS (config)# ip pim version 2</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip pim component</code> - Displays the component information.</li><li>• <code>show ip pim interface</code> - Displays the router's PIM interfaces.</li><li>• <code>show ip pim interface df</code> - Displays the df states of all the PIM interfaces.</li></ul>

## 38.4 set ip pim threshold

---

<b>Command Objective</b>	This command configures the Shortest Path Tree (SPT) group or source threshold. To switch to SPT, the threshold must be configured.
<b>Syntax</b>	<code>set ip pim threshold { spt-grp   spt-src } &lt; number of packets (0-2147483647)&gt;</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>spt-grp</code> - Initiates the source specific counters for a particular group when the threshold of data rate for any group exceeds. It is based on number of packets.</li><li>• <code>spt-src</code> - Initiates the switching to shortest path tree when the threshold of data rate for any source exceeds. It is based on number of packets.</li><li>• <code>&lt; number of packets (0-2147483647)&gt;</code> - Specifies the number of registered packets received. This value ranges from 0 to 2147483647.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	0
<b>Note:</b>	This command executes only if PIM or PIMv6 module is enabled globally.
<b>Example</b>	<code>SEFOS (config)# set ip pim threshold spt-grp 50</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip pim / ip multicast</code> - Enables or disables the PIM globally.</li><li>• <code>set ipv6 pim</code> - Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>set ip pim spt-switchperiod</code> - Configures the time period (in seconds) over which the data rate is to be monitored for switching to shortest path tree.</li><li>• <code>show ip pim thresholds</code> - Displays threshold configured for SPT, RP thresholds, and rate limit values for both SM.</li></ul>

---

## 38.5 set ip pim spt-switchperiod

---

**Command Objective** This command configures the time period (in seconds) over which the data rate is to be monitored for switching to shortest path tree. This value ranges from 0 to 2147483647.

The same period is used for monitoring the data rate for both source and group. To switch to SPT, this period must be configured. The SPT is used for multicast transmission of packets with the shortest path from sender to recipients.

---

**Syntax** `set ip pim spt-switchperiod <0-2147483647 (in secs)>`

---

**Mode** Global Configuration Mode

---

**Package** Enterprise and Metro\_E

---

**Default** 0 seconds

---

Note: This command executes only if PIM or PIMv6 module is enabled globally.

---

**Example** `SEFOS (config)# set ip pim spt-switchperiod 60`

---

**Related Command(s)**

- `set ip pim / ip multicast` - Enables or disables the PIM globally.
- `set ipv6 pim` - Enables or disables PIMv6 feature in the switch globally.
- `show ip pim thresholds` - Displays threshold configured for SPT, RP thresholds, and rate limit values for both SM and DM.

---



## 38.6 set ip pim rp-threshold

---

**Command Objective** This command configures the threshold at which the RP (Rendezvous Point) initiates switching to source specific shortest path tree. This value ranges from 0 to 2147483647.

To switch to SPT, this threshold must be configured. The switching is based on the number of registered packets received.

---

**Syntax** `set ip pim rp-threshold <0-2147483647 (number of reg packets)>`

---

**Mode** Global Configuration Mode

---

**Package** Enterprise and Metro\_E

---

**Default** 0

---

Note: This command executes only if PIM or PIMv6 module is enabled globally.

---

**Example** `SEFOS (config)# set ip pim rp-threshold 50`

---

**Related Command(s)**

- `set ip pim / ip multicast` – Enables or disables the PIM globally.
- `set ipv6 pim` – Enables or disables PIMv6 feature in the switch globally.
- `show ip pim thresholds` – Displays threshold configured for SPT, RP thresholds, and rate limit values for both SM and DM.

---

## 38.7 set ip pim rp-switchperiod

---

**Command Objective** This command configures the time period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree. This value ranges from 0 to 2147483647.

RP-tree is a pattern in which multicast packets are sent to a PIM-SM router by unicast and then forwarded to actual recipients from RP. To switch to SPT, this period must be configured.

---

**Syntax** `set ip pim rp-switchperiod <0-2147483647(in secs)>`

---

**Mode** Global Configuration Mode

---

**Package** Enterprise and Metro\_E

---

**Default** 0 seconds

---

Note: This command executes only if PIM or PIMv6 module is enabled globally.

---

**Example** `SEFOS (config)# set ip pim rp-switchperiod 100`

---

**Related Command(s)**

- `set ip pim / ip multicast` – Enables or disables the PIM globally.
- `set ipv6 pim` – Enables or disables PIMv6 feature in the switch globally.
- `show ip pim thresholds` – Displays threshold configured for SPT, RP thresholds, and rate limit values for both SM.

---

## 38.8 set ip pim regstop-ratelimit-period

---

**Command Objective** This command configures the period over which RP monitors the number of register packets after sending the register stop message. This value ranges from 0 to 2147483647.

Register stop message is used to avoid encapsulation of multicast data packets from the first hop router to the RP.

---

**Syntax** `set ip pim regstop-ratelimit-period <0-2147483647 (in secs)>`

---

**Mode** Global Configuration Mode

---

**Package** Enterprise and Metro\_E

---

**Default** 5 seconds

---

Note: This command executes only if PIM or PIMv6 module is enabled globally.

---

**Example** `SEFOS (config)# set ip pim regstop-ratelimit-period 100`

---

**Related Command(s)**

- `set ip pim / ip multicast` - Enables or disables the PIM globally.
- `set ipv6 pim` - Enables or disables PIMv6 feature in the switch globally.
- `show ip pim thresholds` - Displays threshold configured for SPT, RP thresholds, and rate limit values for both SM.

---

## 38.9 set ip pim pmbr

---

<b>Command Objective</b>	<p>This command enables or disables the PIM Multicast Border Router (PMBR) Status.</p> <p>A PMBR integrates two different PIM domains (either PIM-SM or PIM-DM) and also connects a PIM domain to other multicast routing domain(s).</p>
<b>Syntax</b>	<pre>set ip pim pmbr { enable   disable }</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>enable</b> - Enables the PMBR status.</li><li>• <b>disable</b> - Disables the PMBR status.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	Disable
	<p><u>Note:</u> This command executes only if PIM or PIMv6 module is enabled globally.</p>
<b>Example</b>	<pre>SEFOS (config)# set ip pim pmbr enable</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>set ip pim / ip multicast</b> - Enables or disables the PIM globally.</li><li>• <b>set ipv6 pim</b> - Enables or disables PIMv6 feature in the switch globally.</li><li>• <b>show ip pim thresholds</b> - Displays threshold configured for SPT, RP thresholds, and rate limit values for both SM.</li><li>• <b>ip pim external border</b> - Sets the external non-PIM domain BSR message border for an interface which stops the BSR message forwarding over the specified interface.</li></ul>

---

## 38.10 ip pim component

---

**Command Objective** This command configures the PIM component in the router and enters into PIM component mode. The PIM component corresponds to each instance of a PIM domain and classifies it as Sparse or Dense mode.

The no form of the command destroys the PIM component. This value ranges from 2 to 255.

The PIM Component 1 cannot be deleted as it is the default component.

---

**Syntax** `ip pim component <ComponentId (1-255)> [Scope-zone-name (64) ]`

`no ip pim component <ComponentId (2-255)>`

---

**Parameter Description**

- `<ComponentId (1-255)>` - Configures the PIM component in the router and enters into PIM component mode. This value ranges from 1 to 255.
- `Scope-zone-name (64)` - Configures the scope-zone-name. The maximum length of the string is 64. To configure the scope-zone name, scope-zone should be created in the interface. Scope is a 4-bit value that describes the scope of an IPv6 address. A unicast address can possibly have 2 scopes (Linklocal and Global) only and a multicast address can have a maximum of 11 scopes. The scope zone name should be the same as that of the zone created in the `ipv6 scope-zone` command. If `ipv6 scope-zone` is created as `scopeA 1`, then the scope zone name should be `scopeA1` (without space).

---

**Mode** Global Configuration Mode

---

**Package** Enterprise and Metro\_E

---

**Default**

- Component-Id - 1

---

Note: This command executes only if PIM or PIMv6 module is enabled globally.

---

**Example**

```
SEFOS (config)# ip pim component 1

SEFOS (pim-comp)#
```

---

**Related Command(s)**

- `set ip pim / ip multicast` - Enables or disables the PIM globally.
- `set ipv6 pim` - Enables or disables PIMv6 feature in the switch globally.
- `ipv6 scope-zone` - Creates IPv6 scope zone on an interface.

---

- 
- `show ip pim component` - Displays the component information.
  - `set ip pim graft-retry interval` - Configures the time before which graft is retransmitted upon no receipt of Graft ACK.
  - `set ipv6 pim graft-retry interval` - Configures the time before which graft is retransmitted upon no receipt of Graft ACK.
  - `show ip pim interface df` - Displays the df states of all the PIM interfaces.
-

## 38.11 set ip pim static-rp

---

<b>Command Objective</b>	This command enables or disables the static RP configuration status. This command specifies whether to use the configured static RP.
<b>Syntax</b>	<code>set ip pim static-rp { enable   disable }</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>enable</code> - Enables the Static RP configuration status.</li><li>• <code>disable</code> - Disables the Static RP configuration status.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	Disable
	<u>Note:</u> This command executes only if PIM or PIMv6 module is enabled globally.
<b>Example</b>	<code>SEFOS (config)# set ip pim static-rp enable</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip pim / ip multicast</code> - Enables or disables the PIM globally.</li><li>• <code>set ipv6 pim</code> - Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>show ip pim rp-set</code> - Displays the RP-set information.</li><li>• <code>show ip pim rp-static</code> - Displays the RP-static information.</li><li>• <code>show ip pim interface df</code> - Displays the df states of all the PIM interfaces.</li></ul>

---

## 38.12 set ip pim state-refresh origination-interval

---

**Command Objective** This command configures the interval between successive SRM (State Refresh Messages) control messages originated and sent out by the router. This value ranges from 4 to 100. The no form of the command disables origination (generation) of SRM control messages by the router.

This command is useful if the router is the first-hop router, that is, the source is directly connected.

---

**Syntax** `set ip pim state-refresh origination-interval [<4-100>]`  
`no ip pim state-refresh origination-interval`

---

**Mode** Global Configuration Mode

---

**Package** Enterprise and Metro\_E

---

**Default** 60 seconds

---

Note: This command executes only if PIM or PIMv6 module is enabled globally.

---

**Example** `SEFOS(config)# set ip pim state-refresh origination-interval 50`

---

**Related Command(s)**

- `set ip pim / ip multicast` - Enables or disables the PIM globally.
- `set ipv6 pim` - Enables or disables PIMv6 feature in the switch globally.
- `show ip pim interface detail` - Displays the router's PIM interfaces.

---



## 38.13 ip pim state-refresh disable

---

<b>Command Objective</b>	<p>This command disables the SRM processing and forwarding, that is, the router drops the State Refresh Messages, if received, and also the router will not advertise the SR Capability in hello messages.</p> <p>The no form of the command enables the SRM processing and forwarding. On enabling, this router advertises itself as SR Capable in hello Messages.</p>
<b>Syntax</b>	<pre>ip pim state-refresh disable</pre> <pre>no ip pim state-refresh disable</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	SRM processing and forwarding is enabled.
	<p><u>Note:</u> This command executes only if PIM or PIMv6 module is enabled globally.</p>
<b>Example</b>	<pre>SEFOS(config)# ip pim state-refresh disable</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip pim / ip multicast</code> - Enables or disables the PIM globally.</li><li>• <code>set ipv6 pim</code> - Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>show ip pim interface detail</code> - Displays the router's PIM interfaces.</li></ul>

---

## 38.14 set ip pim source-active interval

---

**Command Objective** This command configures the time duration for which the SRM control messages would be originated by the router after a data packet is received. The no form of the command sets the source active interval to its default value.

This command is useful if the router is the first-hop router, that is, the source is directly connected.

---

**Syntax** `set ip pim source-active interval <120-210>`  
`no ip pim source-active interval`

---

**Mode** Global Configuration Mode

---

**Package** Enterprise and Metro\_E

---

**Default** 210 seconds

---

Note: This command executes only if PIM or PIMv6 module is enabled globally.

---

**Example** `SEFOS(config)# set ip pim source-active interval 150`

---

**Related Command(s)**

- `set ip pim / ip multicast` - Enables or disables the PIM globally.
- `set ipv6 pim` - Enables or disables PIMv6 feature in the switch globally.
- `show ip pim mroute` - Displays the PIM multicast information.

---

## 38.15 set mode

<b>Command Objective</b>	This command sets the component mode to sparse or dense.
<b>Syntax</b>	<code>set mode {sparse   dense}</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>sparse</b> - Indicates the component is running in Sparse mode, explicitly building unidirectional shared trees rooted at a rendezvous point (RP) per group, and optionally creates shortest-path trees per source.</li><li>• <b>dense</b> - Indicates the component is running in Dense mode, implicitly building shortest-path trees by flooding multicast traffic domain wide, and then pruning back branches of the tree where no receivers are present.</li></ul>
<b>Mode</b>	PIM Component Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	sparse
<b>Note:</b>	This command executes only if PIM or PIMv6 module is enabled globally.
<b>Example</b>	<code>SEFOS(pim-comp)# set mode dense</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip pim / ip multicast</code> - Enables or disables the PIM globally.</li><li>• <code>set ipv6 pim</code> - Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>ip pim component</code> - Configures the PIM component in the router and enters into PIM component mode.</li><li>• <code>set ip pim graft-retry interval</code> - Configures the time before which graft is retransmitted upon no receipt of Graft ACK.</li><li>• <code>set ipv6 pim graft-retry interval</code> - Configures the time before which graft is retransmitted upon no receipt of Graft ACK.</li><li>• <code>show ip pim component</code> - Displays the component information.</li><li>• <code>show ip pim interface df</code> - Displays the df states of all the PIM interfaces.</li></ul>

## 38.16 rp-candidate rp-address

---

**Command Objective** This command configures the address of the interface, which will be advertised as a Candidate-RP.

A Candidate-RP is a router configured to send periodic Candidate-RP-Advertisement messages to the BSR, and processes Join, Prune, or Register messages for the advertised group prefix, when it is elected as RP.

The no form of the command disables the address of the interface, which will be advertised as a Candidate-RP.

---

**Syntax**

```
rp-candidate rp-address <Group Address> <Group Mask> <IP address> [Priority <0-255>] [bidir]
```

```
no rp-candidate rp-address <Group Address> <Group Mask> <RP address>
```

---

**Parameter Description**

- **<Group Address>** - Configures the IP multicast group address for which the entry contains multicast routing information.
- **<Group Mask>** - Configures the IP multicast group address mask that gives the group prefix for which the entry contains information about the RP.
- **<IP address>** - Configures the IP address.
- **Priority <0-255>** - Configures the priority of the candidate RP. This value ranges from 0 to 255.
- **bidir** - Configures bidirectional status of RP. Bidirectional PIM is an extension of PIM-SM, where multicast traffic can flow in both directions. All sources are potential receivers also.

---

**Mode** PIM Component Mode

---

**Package** Enterprise and Metro\_E

---

Note: This command executes only if,

- PIM module is enabled globally.
  - PIM mode is set as sparse.
  - PIM query interval and IP address is configured.
  - Bidirectional PIM should be enabled to use the bidir option.
-

---

**Example**

```
SEFOS(pim-comp)# rp-candidate rp-address 224.1.0.0  
255.255.0.0 20.0.0.2 bidir
```

---

**Related Command(s)**

- **set ip pim/ ip multicast** - Enables or disables PIM feature in the switch globally.
  - **set mode** - Sets the component mode to sparse or dense.
  - **ip address** - Sets the IP address for an interface.
  - **ip pim bidir-enable** - Enables bidirectional PIM feature.
  - **ip pim component** - Configures the PIM component in the router and enters into PIM component mode.
  - **ip pim componentId** - Adds the interface to the PIM component.
  - **ip pim query-interval** - Configures the frequency at which PIM hello messages are transmitted on the interface.
  - **ip pim bsr-candidate - value** - Sets the preference value for the local interface as a candidate bootstrap router.
  - **ip pim bsr-candidate - VLAN** - Sets the local interface as a candidate bootstrap router.
  - **show ip pim interface** - Displays the router's PIM interfaces.
  - **show ip pim rp-set** - Displays the RP-set information.
  - **show ip pim rp-candidate** - Displays the RP-candidate information.
  - **show ip pim rp-hash** - Displays the elected RP for the multicast group address with the mask length.
  - **show ip pim interface df** - Displays the df states of all the PIM interfaces.
-

## 38.17 rp-candidate holdtime

---

**Command Objective** This command configures the holdtime of the component when it is a candidate RP in the local domain. This value ranges from 0 to 255. Holdtime is the amount of time that the candidate RP advertisement is valid. This field allows advertisements to be aged out.

The no form of the command sets the holdtime of the component to its default value which indicates that the local system is not a candidate RP.

---

**Syntax** `rp-candidate holdtime <Holdtime value (0-255)>`  
`no rp-candidate holdtime`

---

**Mode** PIM Component Mode

---

**Package** Enterprise and Metro\_E

---

**Default** 0

---

Note: This command executes only if,

- PIM module is enabled globally.
- PIM mode is set as sparse.

---

**Example** `SEFOS (pim-comp) # rp-candidate holdtime 25`

---

**Related Command(s)**

- `set ip pim/ ip multicast` - Enables or disables PIM feature in the switch globally.
- `set mode` - Sets the component mode to sparse or dense.
- `show ip pim rp-candidate` - Displays the RP-candidate information.
- `show ip pim rp-hash` - Displays the elected RP for the multicast group address with the mask length.
- `show ip pim interface df` - Displays the df states of all the PIM interfaces.

---

## 38.18 rp-static rp-address

---

**Command Objective** This command configures the address of the interface, which will be advertised as a Static-RP.

Static configuration allows additional structuring of the multicast traffic by directing the multicast join or prune messages to statically configured RPs.

The no form of the command disables the address of the interface, which will be advertised as a Static-RP.

---

**Syntax** `rp-static rp-address <Group Address> <Group Mask> <IP address> [bidir]`

`no rp-static rp-address <Group Address> <Group Mask>`

---

**Parameter Description**

- **<Group Address>** - Configures the PIM Sparse multicast group address using the listed RP.
- **<Group Mask>** - Configures the IP multicast group address mask that gives the group prefix for which the entry contains information about the RP.
- **<IP address>** - Configures the IP address.
- **bidir** - Configures the bidirectional status of the RP. Bidirectional PIM is an extension of PIM-SM, where multicast traffic can flow in both directions. All sources are potential receivers also.

---

**Mode** PIM Component Mode

---

**Package** Enterprise and Metro\_E

---

Note: This command executes only if,

- PIM module is enabled globally.
- PIM mode is set as sparse.
- Bidirectional PIM should be enabled to use the bidir option.

---

**Example** `SEFOS (pim-comp) # rp-static rp-address 224.1.0.0  
255.255.0.0 20.0.0.2 bidir`

---

**Related Command(s)**

- `set ip pim/ ip multicast` - Enables or disables PIM feature in the switch globally.

---

- 
- **set mode** - Sets the component mode to sparse or dense.
  - **ip pim bidir-enable** – Enables bidirectional PIM feature.
  - **ip pim component** – Configures the PIM component in the router and enters into PIM component mode.
  - **ip pim componentId** – Adds the interface to the PIM component.
  - **show ip pim rp-static** – Displays the RP-static information.
  - **show ip pim rp-hash** - Displays the elected RP for the multicast group address with the mask length.
  - **show ip pim interface** - Displays the router's PIM interfaces.
  - **show ip pim interface df** - Displays the df states of all the PIM interfaces.
-



## 38.19 ip pim query-interval

---

<b>Command Objective</b>	<p>This command enables PIM over an interface and configures the frequency at which PIM hello messages are transmitted on this interface. This value ranges from 0 to 65535.</p> <p>The query message informs the presence of a PIM router on the interface to the neighboring PIM routers.</p> <p>The no form of the command sets the default hello timer interval for this interface.</p>
<b>Syntax</b>	<pre>ip pim query-interval &lt;Interval (0-65535) secs&gt;  no ip pim query-interval</pre>
<b>Mode</b>	Interface Configuration Mode (VLAN / Router)
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	30 seconds
	<p><u>Note:</u> This command executes only if PIM module is enabled globally.</p>
<b>Example</b>	<p><b>Interface Configuration Mode (VLAN)</b></p> <pre>SEFOS(config)# interface vlan 3 SEFOS (config-if)# ip pim query-interval 60</pre> <p><b>Interface Configuration Mode (Router)</b></p> <pre>SEFOS(config)# interface extreme-ethernet 0/2 SEFOS(config-if)# no switchport SEFOS (config-if)# ip pim query-interval 60</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip pim/ ip multicast</code> - Enables or disables PIM feature in the switch globally.</li><li>• <code>rp-static rp-address</code> - Configures the address of the interface, which will be advertised as a Static-RP.</li><li>• <code>show ip pim interface</code> - Displays the routers PIM interfaces.</li></ul>

---

## 38.20 ip pim message-interval

---

**Command Objective** This command configures the frequency at which PIM Join or Prune messages are transmitted on the PIM interface. This value ranges from 0 to 65535.

The same Join or Prune message interval must be used on all the PIM routers in the PIM domain. If all the routers do not use the same timer interval, the performance of PIM Sparse can be adversely affected.

The no form of the command resets the PIM Join or Prune message to its default value.

---

**Syntax** `ip pim message-interval <Interval(0-65535)>`  
`no ip pim message-interval`

---

**Mode** Interface Configuration Mode (VLAN/Router)

---

**Package** Enterprise and Metro\_E

---

**Default** 60

---

Note: This command executes only if PIM module is enabled globally.

---

**Example** **Interface Configuration Mode (VLAN)**

```
SEFOS(config)# interface vlan 3
SEFOS (config-if)# ip pim message-interval 120
```

**Interface Configuration Mode (Router)**

```
SEFOS(config)# interface extreme-ethernet 0/2
SEFOS (config-if)# no switchport
SEFOS (config-if)# ip pim message-interval 120
```

---

**Related Command(s)**

- `set ip pim/ ip multicast` - Enables or disables PIM feature in the switch globally.
- `show ip pim interface` - Displays the routers PIM interfaces.

---

## 38.21 ip pim bsr-candidate - value

---

**Command Objective** This command configures the preference value for the local interface as a candidate Bootstrap Router (BSR). This preference value ranges between 0 and 255.

A BSR is a dynamically elected router within a PIM domain. The router with highest priority is considered as the BSR. If the priority values are same, then the router with largest IP address is considered as the BSR.

The no form of the command resets the default preference value for the local interface as a candidate bootstrap router.

---

**Syntax** `ip pim bsr-candidate <value (0-255)>`  
`no ip pim bsr-candidate`

---

**Mode** Interface Configuration Mode (VLAN/Router)

---

**Package** Enterprise and Metro\_E

---

**Default** 0

---

Note: This command executes only if PIM module is enabled globally.

---

**Example** **Interface Configuration Mode (VLAN)**

```
SEFOS(config)# interface vlan 3
SEFOS (config-if)# ip pim bsr-candidate 1
```

**Interface Configuration Mode (Router)**

```
SEFOS(config)# interface extreme-ethernet 0/2
SEFOS (config-if)# no switchport
SEFOS (config-if)# ip pim bsr-candidate 1
```

---

**Related Command(s)**

- `set ip pim/ ip multicast` - Enables or disables PIM feature in the switch globally.
- `rp-candidate rp-address` - Sets the address of the interface, which will be advertised as a Candidate-RP.
- `show ip pim bsr` - Displays the BSR information.
- `show ip pim interface df` - Displays the df states of all the PIM

---

---

interfaces.

---

## 38.22 ip pim bsr-candidate – vlan

---

<b>Command Objective</b>	<p>This command configures the local interface as a candidate Bootstrap Router (BSR).</p> <p>A BSR is a dynamically elected router within a PIM domain. The router with highest priority is considered as the BSR. If the priority values are same, then the router with largest IP address is considered as the BSR.</p> <p>This command is a standardized implementation of the existing command <code>ip pim bsr-candidate - value</code>. Its operation is similar to the existing command.</p>
<b>Syntax</b>	<pre>ip pim bsr-candidate &lt;vlan-interface-no (1-4094)&gt; [&lt;hash-mask-length&gt;] [priority &lt;value (0-255)&gt;]</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>&lt;vlan-interface-no (1-4094)&gt;</b> - Configures the VLAN interface number from which BSR address is derived to make BSR a candidate. This value ranges from 1 to 4094.</li><li>• <b>&lt;hash-mask-length&gt;</b> - Configures the length (in bits) of the mask on which an AND operation is performed with the group address before calling the hash function. This value ranges from 0 to 32. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.</li><li>• <b>priority&lt;value (0-255)&gt;</b> - Configures the priority of the candidate BSR. This value ranges from 0 to 255.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	<ul style="list-style-type: none"><li>• hash-mask-length - 30</li><li>• priority - 0</li></ul>
<b>Note:</b>	This command executes only if PIM module is enabled globally.
<b>Example</b>	<pre>SEFOS (config)# ip pim bsr-candidate 1 priority 100</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>set ip pim/ ip multicast</b> - Enables or disables PIM feature in the switch globally.</li><li>• <b>rp-candidate rp-address</b> - Sets the address of the interface, which will be advertised as a Candidate-RP.</li></ul>

---

- 
- `show ip pim bsr` – Displays the BSR information.
-

## 38.23 ip pim componentId

---

<b>Command Objective</b>	<p>This command adds the interface to the PIM component. This value ranges from 1 to 255. This command adds the current VLAN into the specified PIM component.</p> <p>The no form of the command removes the interface from the PIM component.</p>
<b>Syntax</b>	<pre>ip pim componentId &lt;value (1-255)&gt;  no ip pim componentId &lt;value (1-255)&gt;</pre>
<b>Mode</b>	Interface Configuration Mode (VLAN /Router)
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	1
<b>Note:</b>	<p>This command executes only if,</p> <ul style="list-style-type: none"><li>• PIM module is enabled globally.</li><li>• PIM component is configured in the router.</li></ul>
<b>Example</b>	<p><b>Interface Configuration Mode (VLAN)</b></p> <pre>SEFOS(config)# interface vlan 3 SEFOS(config-if)# ip pim componentId 1</pre> <p><b>Interface Configuration Mode (Router)</b></p> <pre>SEFOS(config)# interface extreme-ethernet 0/2 SEFOS(config-if)# no switchport SEFOS (config-if)# ip pim componentId 1</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip pim/ ip multicast</code> - Enables or disables PIM feature in the switch globally.</li><li>• <code>ip pim component</code> - Configures the PIM component in the router.</li><li>• <code>rp-candidate rp-address</code> - Sets the address of the interface, which will be advertised as a Candidate-RP.</li><li>• <code>rp-static rp-address</code> - Sets the address of the interface, which will be advertised as a Static-RP.</li></ul>

---

- 
- `show ip pim interface` – Displays the routers PIM interfaces.
  - `set ip pim graft-retry interval` - Configures the time before which graft is retransmitted upon no receipt of Graft ACK.
  - `show ip pim component` – Displays the component information.
  - `set ipv6 pim graft-retry interval` - Configures the time before which graft is retransmitted upon no receipt of Graft ACK.
-



## 38.24 ip pim dr-priority

---

**Command Objective** This command configures the designated router priority value configured for the router interface. This value ranges from 1 to 4294967295.

The no form of the command sets the default designated router priority value for the router interface.

The DR sets up multicast route entries and sends corresponding Join, Prune and, Register messages on behalf of directly-connected receivers and sources, respectively.

---

**Syntax** `ip pim dr-priority <priority>`

`no ip pim dr-priority`

---

**Mode** Interface Configuration Mode (VLAN /Router)

---

**Package** Enterprise and Metro\_E

---

**Default** 1

---

Note: This command executes only if PIM module is enabled globally.

---

**Example** **Interface Configuration Mode (VLAN)**

```
SEFOS(config)# interface vlan 3
SEFOS(config-if)# ip pim dr-priority 100
```

**Interface Configuration Mode (Router)**

```
SEFOS(config)# interface extreme-ethernet 0/2
SEFOS(config-if)# no switchport
SEFOS (config-if)# ip pim dr-priority 100
```

---

**Related Command(s)**

- `set ip pim/ ip multicast` - Enables or disables PIM feature in the switch globally.
- `show ip pim interface` - Displays the routers PIM interfaces.

---

## 38.25 ip pim override-interval

---

**Command Objective** This command configures the override interval configured for router interface. This value ranges from 0 to 65535.

Override interval is the random amount of time delay for sending override messages. The purpose of override interval is to avoid synchronization of override messages when multiple downstream routers share a multi-access link.

The no form of the command sets the default override interval for router interface.

---

**Syntax** `ip pim override-interval <interval(0-65535)>`  
`no ip pim override-interval`

---

**Mode** Interface Configuration Mode (VLAN /Router)

---

**Package** Enterprise and Metro\_E

---

**Default** 0

---

Note: This command executes only if PIM module is enabled globally.

---

**Example** **Interface Configuration Mode (VLAN)**  
`SEFOS (config)# interface vlan 3`  
`SEFOS (config-if)# ip pim override-interval 100`  
**Interface Configuration Mode (Router)**  
`SEFOS (config)# interface extreme-ethernet 0/2`  
`SEFOS (config-if)# no switchport`  
`SEFOS (config-if)# ip pim override-interval 100`

---

**Related Command(s)**

- `set ip pim/ ip multicast` - Enables or disables PIM feature in the switch globally.
- `show ip pim interface` - Displays the routers PIM interfaces.

---

## 38.26 ip pim lan-delay

---

**Command Objective** This command configures the LAN Delay configured for the router interface. This value ranges from 0 to 65535.

The LAN Delay inserted by a router in the LAN Prune Delay option performs the expected message propagation delay on the interface. It is used by upstream routers to find the delayed time interval for a Join override message before pruning an interface.

The no form of the command sets the default LAN Delay for the router per interface.

---

**Syntax** `ip pim lan-delay <value(0-65535)>`  
`no ip pim lan-delay`

---

**Mode** Interface Configuration Mode (VLAN /Router)

---

**Package** Enterprise and Metro\_E

---

**Default** 0

---

Note: This command executes only if PIM module is enabled globally.

---

**Example** **Interface Configuration Mode (VLAN)**  
`SEFOS(config)# interface vlan 3`  
`SEFOS(config-if)# ip pim lan-delay 120`  
**Interface Configuration Mode (Router)**  
`SEFOS(config)# interface extreme-ethernet 0/2`  
`SEFOS(config-if)# no switchport`  
`SEFOS (config-if)# ip pim lan-delay 120`

---

**Related Command(s)**

- `set ip pim/ ip multicast` - Enables or disables PIM feature in the switch globally.
- `set ip pim lan-prune-delay` - Enables or disables the LanPruneDelay.
- `show ip pim interface` - Displays the routers PIM interfaces.

---

## 38.27 set ip pim lan-prune-delay

---

<b>Command Objective</b>	This command enables or disables the LanPruneDelay bit configured for the router interface to advertise the LAN delay. The command specifies whether to use LAN prune delay or not.
<b>Syntax</b>	<code>set ip pim lan-prune-delay { enable   disable }</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>enable</code> - Enables LAN-prune-delay.</li><li>• <code>disable</code> - Disables LAN-prune-delay.</li></ul>
<b>Mode</b>	Interface Configuration Mode (VLAN /Router)
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	disable
<b>Note:</b>	This command executes only if PIM module is enabled globally.
<b>Example</b>	<pre>Interface Configuration Mode (VLAN) SEFOS(config)# interface vlan 3 SEFOS(config-if)# set ip pim lan-prune-delay enable  Interface Configuration Mode (Router) SEFOS(config)# interface extreme-ethernet 0/2 SEFOS(config-if)# no switchport SEFOS (config-if)# set ip pim lan-prune-delay enable</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip pim/ ip multicast</code> - Enables or disables PIM feature in the switch globally.</li><li>• <code>ip pim lan-delay</code> - Configures the LanDelay configured for the router interface.</li><li>• <code>show ip pim interface</code> - Displays the routers PIM interfaces.</li></ul>

---

## 38.28 set ip pim graft-retry interval

---

**Command Objective** This command configures the time before which graft is retransmitted upon no receipt of Graft ACK. This value ranges from 1 to 10.

The no form of the command sets the graft retry interval to its default value.

---

**Syntax** `set ip pim graft-retry interval <value(1-10)>`

`no ip pim graft-retry interval`

---

**Mode** Interface Configuration Mode (VLAN /Router)

---

**Package** Enterprise and Metro\_E

---

**Default** 3 seconds

---

Note: This command executes only if PIM module is enabled globally.

To configure the graft-retry interval, the PIM component that the interface is mapped to should be in dense mode.

---

**Example** **Interface Configuration Mode (VLAN)**

```
SEFOS(config)# interface vlan 3
```

```
SEFOS(config-if)# set ip pim graft-retry interval 4
```

**Interface Configuration Mode (Router)**

```
SEFOS(config)# interface extreme-ethernet 0/2
```

```
SEFOS(config-if)# no switchport
```

```
SEFOS(config-if)# set ip pim graft-retry interval 4
```

---

**Related Command(s)**

- `set ip pim/ ip multicast` - Enables or disables PIM feature in the switch globally.
  - `set mode` - Sets the component mode to sparse or dense.
  - `ip pim componentId` - Adds the interface to the PIM component.
  - `show ip pim interface detail` - Displays the router's PIM interfaces.
-

## 38.29 no ip pim interface

---

<b>Command Objective</b>	This command deletes an interface at PIM level. This command is used to destroy the interface at PIM.
<b>Syntax</b>	<code>no ip pim interface</code>
<b>Mode</b>	Interface Configuration Mode (VLAN/Router)
<b>Package</b>	Enterprise and Metro_E
<u>Note:</u>	This command executes only if PIM module is enabled globally.
<b>Example</b>	<p><b>Interface Configuration Mode (VLAN)</b></p> <pre>SEFOS (config)# interface vlan 3 SEFOS (config-if)# no ip pim interface</pre> <p><b>Interface Configuration Mode (Router)</b></p> <pre>SEFOS (config)# interface extreme-ethernet 0/3 SEFOS (config-if)# no switchport SEFOS (config-if)# no ip pim interface</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip pim/ ip multicast</code> - Enables or disables PIM feature in the switch globally.</li><li>• <code>show ip pim interface</code> - Displays the routers PIM interfaces.</li></ul>

---

## 38.30 debug ip pim

---

<b>Command Objective</b>	<p>This command enables the tracing of the PIM module as per the configured debug levels. The trace statements are generated for the configured trace levels.</p> <p>This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.</p> <p>A four byte integer value is specified for enabling the level of debugging. Each bit in the four byte integer variable represents a level of debugging. The combination of levels is also allowed. The user has to enter the corresponding integer value for the bit set.</p> <p>The no form of the command disables the tracing of the PIM module as per the configured debug levels. The trace statements are not generated for the configured trace levels.</p>
--------------------------	---

---

<b>Syntax</b>	<pre>debug ip pim {[nbr][grp][jp][ast][bsr][io] [pnbr][mrt][mdh][mgmt] [srm][red][df][bmrt]   [all]}  no debug ip pim {[nbr][grp][jp][ast][bsr][io][pnbr][mrt][mdh][mgmt] [srm][red][df][bmrt]   [all]}</pre>
---------------	---

---

<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>nbr</b> - Sets the module as PIM Neighbor Discovery module, for which the tracing is to be done as per the configured debug levels.</li><li>• <b>grp</b> - Generates debug statements for group membership traces.</li><li>• <b>jp</b> - Generates debug statements for Join or Prune traces.</li><li>• <b>ast</b> - Generates debug statements for assert state traces.</li><li>• <b>bsr</b> - Generates debug statements for Bootstrap or RP traces.</li><li>• <b>io</b> - Generates debug statements for input and output traces.</li><li>• <b>pnbr</b> - Generates debug statements for interoperability traces.</li><li>• <b>mrt</b> - Generates debug statements for Multicast Route Table Update traces.</li><li>• <b>mdh</b> - Generates debug statements for Multicast Data Handling traces.</li><li>• <b>mgmt</b> - Generates debug statements for management traces.</li></ul>
------------------------------	--

---

- **srm** - Generates debug statements for state refresh messages.
- **red** - Sets the module as PIM redundancy module, for which the tracing is to be done as per the configured debug levels.
- **df** - Generates debug statements for Bidir DF traces.
- **bmr** - Generates debug statements for Bidir routing utility traces.
- **all** - Generates debug statements for all kinds of traces.

**Mode** Privileged EXEC Mode

**Package** Enterprise and Metro\_E

Note: This command executes only if PIM module is enabled globally.

**Example** SEFOS # debug ip pim all

**Related Command(s)**

- **set ip pim/ ip multicast** - Enables or disables PIM feature in the switch globally.
- **show ip pim interface** – Displays the routers PIM interfaces.



## 38.31 show ip pim interface

---

**Command Objective** This command displays the router's PIM interfaces. The information contains the list of interface addresses, the mode of the interface, designated router on that interface, hello interval, Join or Prune interval of the interface, bidirectional status, offer limit, and offer interval.

---

**Syntax** `show ip pim interface [{ Vlan <vlan-id/vfi-id> [df] | <interface-type> <interface-id> [df] | <IP-interface-type> <IP-interface-number> | detail }]`

---

**Parameter Description**

- **vlan <vlan-id/vfi-id>** - Displays PIM configurations for the specified VLAN / VFI ID. This value ranges from 1 to 65535.
  - **<vlan -id>** - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.
  - **<vfi-id>** - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.

---

Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.

Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.

Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.

---

- **<interface-type>** - Displays PIM configurations for the specified type of interface. The interface can be:
  - **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
  - **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gigabits per second.
  - **i-lan** – Internal LAN created on a bridge per IEEE 802.1ap.
- **<interface-id>** - Displays PIM configurations for the specified interface identifier. This is a unique value that represents the specific interface. This

value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan is provided, for interface type i-lan. For example: 1 represents i-lan.

- **<IP-interface-type>** - Display PIM configuration for the specified L3 pseudowire interface in the system.
- **<IP-interface-number>** - Display PIM configuration for the specified L3 pseudowire interface identifier. This is a unique value that represents the specific interface. This value ranges from 1 to 65535 for pseudowire interface.

---

Note: Maximum number of pseudowire interfaces supported in the system is 100.

---

- **df** - Displays the Bidir-PIM Designated Forwarder (DF) related information.
- **detail** - Displays the detailed PIM information for the interface.

---

**Mode** Privileged EXEC Mode

---

**Package** Enterprise and Metro\_E

---

Note: This command executes only if PIM module is enabled globally.

---

**Example**

```
SEFOS# show ip pim interface
Address IfName/IfId Ver/Mode Nbr Qry DR-Address DR-
Prio
                                Count Interval
10.0.0.1 vlan1/160 2/Sparse 0 45 10.0.0.1 5
20.0.0.1 vlan2/33 2/Sparse 0 30 20.0.0.1 1
30.0.0.1 vlan3/34 2/Sparse 0 60 30.0.0.1 1

SEFOS# show ip pim interface vlan 1
Address IfName/IfId Ver/Mode Nbr Qry DR-Address DR-
Prio
                                Count Interval
10.0.0.1 vlan1/160 2/Sparse 0 45 10.0.0.1 5

SEFOS# show ip pim interface detail
vlan1 73 is up
  Internet Address is 11.0.0.1
  Multicast Switching : Enabled
  PIM : Enabled
  PIMv6 : Enabled
  PIM version : 2, mode: Sparse
```

```

PIM DR : 11.0.0.1
PIM DR Priority : 1
PIM Neighbour Count : 0
PIM Hello/Query Interval : 30
PIM Message Interval : 60
PIM Override Interval : 0
PIM Lan Delay : 0
PIM Lan-Prune-Delay : Disabled
PIM Component Id : 1
PIM domain border : disabled
PIM RPF Status : Disabled
PIM Bidirectional Status : Enabled
Offer Interval : 100, Offer Limit : 4

```

**SEFOS# show ip pim interface vlan 1 df**

RP Address	DF Winner	State	Metric	Metric	Pref
20.0.0.0	0.0.0.0	Lose	-1	2147483647	

**Related Command(s)**

- **set ip pim/ ip multicast** - Enables or disables PIM feature in the switch globally.
- **ip pim componentId** - Adds the interface to the PIM component.
- **ip pim component** - Configures the PIM component in the router.
- **ip pim version** - Configures version number of the PIM protocol in the switch.
- **ip pim query-interval** - Sets the frequency at which PIM hello messages are transmitted on this interface.
- **ip pim message-interval** - Sets the frequency at which PIM Join or Prune messages are transmitted on this PIM interface.
- **ip pim bsr-candidate - value** - Sets the preference value for the local interface as a candidate bootstrap router.
- **ip pim dr-priority** - Sets the designated router priority value configured for the router interface.
- **ip pim override-interval** - Sets the override interval configured for router interface.
- **ip pim lan-delay** - Sets the LanDelay configured for the router interface.

- 
- **set ip pim lan-prune-delay** – Sets the LanPruneDelay bit configured for the router interface to advertise the LAN delay.
  - **no ip pim interface** – Deletes an interface at PIM level.
  - **debug ip pim** – Enables PIM trace.
  - **rp-candidate rp-address** - Sets the address of the interface, which will be advertised as a Candidate-RP.
  - **ip pim bidir-enable**- Enables the Bidirectional PIM feature.
  - **ip pim bidir-offer-interval** – Configures the Bidir-PIM offer interval in milliseconds.
  - **ip pim bidir-offer-limit** – Configures the Bidir-PIM offer limit.
-

## 38.32 show ip pim neighbor

---

**Command Objective** This command displays the router's PIM neighbors' information. The information contains the neighbor address, the interface used to reach the PIM neighbor, the up time (the time elapsed since this neighbor became the neighbor of the local router), expiry time (the minimum time remaining before this PIM neighbor will be aged out), LAN delay, and override interval.

---

**Syntax** `show ip pim neighbor [{ Vlan <vlan-id/vfi-id> | <interface-type> <interface-id> | <IP-interface-type> <IP-interface-number>}]`

---

**Parameter Description**

- **vlan <vlan-id/vfi-id>** - Displays PIM neighbor configurations for the specified VLAN / VFI ID. This value ranges from 1 to 65535.
  - **<vlan -id>** - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.
  - **<vfi-id>** - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.

---

Note: The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.

Note: VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.

Note: The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.

---

- **<interface-type>** - Displays the router's PIM neighbors' information for the specified type of interface. The interface can be:
  - **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
  - **xl-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gigabits per second.
  - **i-lan** – Internal LAN created on a bridge per IEEE 802.1ap.
- **<interface-id>** - Displays the router's PIM interfaces for the specified

interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan is provided, for interface type i-lan . For example: 1 represents i-lan.

- **<IP-interface-type>** - Display PIM neighbor configuration for the specified L3 pseudowire interface in the system.
- **<IP-interface-number>** - Display PIM neighbor configuration for the specified L3 pseudowire interface identifier. This is a unique value that represents the specific interface . This value ranges from 1 to 65535 for pseudowire interface.

**Note:** Maximum number of pseudowire interfaces supported in the system is 100.

**Mode** Privileged EXEC Mode

**Package** Enterprise and Metro\_E

**Note:** This command executes only if PIM module is enabled globally.

**Example**

```
SEFOS# show ip pim neighbor vlan 1
Neighbour   IfName/Idx Uptime/Expiry Ver DRPri   CompId
Override   LanDelay
Address
Interval
-----
-
12.0.0.2   vlan1/33   00:00:45/275  v2  1       1    0
0
```

**Related Command(s)**

- **set ip pim/ ip multicast** - Enables or disables PIM feature in the switch globally.
- **ip pim component** - Configures the PIM component in the router.
- **ip pim componentId** - Adds the interface to the PIM component.
- **ip pim query-interval** - Configures the frequency at which PIM hello messages are transmitted on this interface.
- **ip pim message-interval** - Configures the frequency at which PIM Join or Prune messages are transmitted on this PIM interface.
- **ip pim bsr-candidate - value** - Configures the preference value for the local interface as a candidate bootstrap router.

## 38.33 show ip pim rp-candidate

<b>Command Objective</b>	This command displays the candidate RP information. The information contains the group addresses, the group mask, and the RP address that indicates the IP address of the Rendezvous Point (RP) for the listed PIM Sparse group.
<b>Syntax</b>	<code>show ip pim rp-candidate [ComponentId &lt;1-255&gt;] [bidir]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>ComponentId &lt;1-255&gt;</code> - Displays the specified Component ID for which the candidate RP information is to be displayed. This value ranges from 0 to 255.</li><li>• <code>bidir</code> - Displays the Bidir-PIM capable groups. Bidirectional PIM is an extension of PIM-SM, where multicast traffic can flow in both directions. All sources are potential receivers also.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Note:</b>	This command executes only if PIM module is enabled globally.
<b>Example</b>	<pre>SEFOS# show ip pim rp-candidate 2 bidir CompId  GroupAddress  Group Mask  RPAddress/Priority   2      224.1.0.0      255.255.0.0  20.0.0.1/192</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip pim/ ip multicast</code> - Enables or disables PIM feature.</li><li>• <code>ip pim component</code> - Configures the PIM component in the router.</li><li>• <code>ip pim componentId</code> - Adds the interface to the PIM component.</li><li>• <code>ip pim bidir-enable</code> - Enables the Bidirectional PIM feature.</li><li>• <code>ip pim bsr-candidate - value / ip pim bsr-candidate - vlan</code> - Configures the local interface as a candidate Bootstrap Router.</li><li>• <code>rp-candidate rp-address</code> - Enables the address of the interface, which will be advertised as a Candidate-RP.</li><li>• <code>rp-candidate holdtime</code> - Sets the hold time of the component when it is a candidate RP in the local domain.</li><li>• <code>rp-static rp-address</code> - Sets the address of the interface, which will be advertised as a Static-RP.</li><li>• <code>show ip pim rp-hash</code> - Displays the elected RP for the multicast group</li></ul>

---

address with the mask length.

---



## 38.34 show ip pim rp-set

<b>Command Objective</b>	This command displays the RP-set information. This information includes details of the group prefix, RP address, hold time, and expiry Time.
<b>Syntax</b>	<code>show ip pim rp-set [rp-address] [bidir]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>rp-address</code> - Displays the IP address of the Rendezvous Point (RP) for the listed PIM Sparse group.</li><li>• <code>bidir</code> - Displays Bidir-PIM capable groups. Bidirectional PIM is an extension of PIM-SM, where multicast traffic can flow in both directions. All sources are potential receivers also.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Note:</b>	This command executes only if PIM module is enabled globally.
<b>Example</b>	<pre>SEFOS# show ip pim rp-set bidir PIM Group-to-RP mappings ----- Group Address: 224.1.0.0  Group Mask: 255.255.0.0 RP: 20.0.0.1 Component-Id: 2 Hold Time: 120, Expiry Time: 00:01:43</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip pim/ ip multicast</code> - Enables or disables PIM feature in the switch globally.</li><li>• <code>ip pim component</code> - Configures the PIM component in the router.</li><li>• <code>ip pim componentId</code> - Adds the interface to the PIM component.</li><li>• <code>ip pim bidir-enable</code> - Enables the Bidirectional PIM feature.</li><li>• <code>ip pim bsr-candidate - value / ip pim bsr-candidate - vlan</code> - Configures the local interface as a candidate Bootstrap Router.</li><li>• <code>rp-candidate rp-address</code> - Enables the address of the interface, which will be advertised as a Candidate-RP.</li><li>• <code>set ip pim static-rp</code> - Enables or disables the Static RP configuration status.</li></ul>

- 
- **rp-candidate holdtime** – Sets the hold time of the component when it is a candidate RP in the local domain.
  - **rp-static rp-address** – Sets the address of the interface, which will be advertised as a Static-RP.
  - **show ip pim rp-hash** - Displays the elected RP for the multicast group address with the mask length.
-

## 38.35 show ip pim bsr

---

**Command Objective** This command displays the BSR information. The component ID value ranges between 1 and 255.

---

**Syntax** `show ip pim bsr [Component-Id (1-255)]`

---

**Mode** Privileged EXEC Mode

---

**Package** Enterprise and Metro\_E

---

Note: This command executes only if PIM module is enabled globally.

---

**Example**

```
SEFOS# show ip pim bsr 1
PIMv2 Bootstrap Configuration For Component 1
-----
This system is the Bootstrap Router (BSR)
  BSR Address: 10.0.0.1
  BSR Priority: 6, Hash Mask Length: 30
```

---

**Related Command(s)**

- `ip pim component` - Configures the PIM component in the router.
- `ip pim componentId` - Adds the interface to the PIM component.
- `set ip pim/ ip multicast` - Enables or disables PIM feature in the switch globally.
- `ip pim bsr-candidate - value` - Sets the preference value for the local interface as a candidate bootstrap router.
- `ip pim bsr-candidate - VLAN` - Sets the local interface as a candidate bootstrap router.

---

## 38.36 show ip pim rp-static

---

<b>Command Objective</b>	This command displays the static RP information. The component ID value ranges between 1 and 255.
--------------------------	---

---

<b>Syntax</b>	<code>show ip pim rp-static [ComponentId &lt;1-255&gt;] [bidir]</code>
---------------	--

---

<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>ComponentId &lt;1-255&gt;</b> - Displays the specified Component ID for which the static RP information is to be displayed. This value ranges from 1 to 255.</li><li>• <b>bidir</b> - Displays the Bidir-PIM capable groups. Bidirectional PIM is an extension of PIM-SM, where multicast traffic can flow in both directions. All sources are potential receivers also.</li></ul>
------------------------------	---

---

<b>Mode</b>	Privileged EXEC Mode
-------------	----------------------

---

<b>Package</b>	Enterprise and Metro_E
----------------	------------------------

---

<u>Note:</u>	This command executes only if PIM module is enabled globally.
--------------	---

---

<b>Example</b>	<pre>SEFOS# show ip pim rp-static 2 bidir Static-RP Enabled   CompId  GroupAddress  Group Mask      RPAddress   2       225.1.0.0      255.255.0.0    20.0.0.1</pre>
----------------	--

---

<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>set ip pim/ ip multicast</b> - Enables or disables PIM feature in the switch globally.</li><li>• <b>ip pim component</b> - Configures the PIM component in the router.</li><li>• <b>ip pim componentId</b> - Adds the interface to the PIM component.</li><li>• <b>ip pim bidir-enable</b>- Enables the Bidirectional PIM feature.</li><li>• <b>rp-candidate holdtime</b> – Sets the hold time of the component when it is a candidate RP in the local domain.</li><li>• <b>rp-static rp-address</b> – Sets the address of the interface, which will be advertised as a Static-RP.</li><li>• <b>shutdown - physical/VLAN/port-channel/tunnel interface</b> - Disables a physical interface, VLAN interface, port-channel interface, tunnel interface, or OOB interface.</li><li>• <b>rp-candidate holdtime</b> – Sets the hold time of the component when it</li></ul>
---------------------------	---

---

---

is a candidate RP in the local domain.

- **ip address** - Configures IP address on the interface.
  - **set ip pim static-rp** – Enables or disables the Static RP configuration status.
  - **rp-static rp-address** - Sets the address of the interface, which will be advertised as a Static-RP.
  - **show ip pim rp-hash** - Displays the elected RP for the multicast group address with the mask length.
-

## 38.37 show ip pim component

---

**Command Objective** This command displays the component information. The component ID value ranges between 1 and 255.

---

**Syntax** `show ip pim component [ComponentId <1-255>]`

---

**Mode** Privileged EXEC Mode

---

**Package** Enterprise and Metro\_E

---

Note: This command executes only if PIM module is enabled globally.

---

**Example** `SEFOS# show ip pim component 1`

PIM Component Information

-----  
Component-Id: 1

PIM Mode: sparse, PIM Version: 2

Elected BSR: 10.0.0.1

Candidate RP Holdtime: 0

---

**Related Command(s)**

- `set ip pim/ ip multicast` - Enables or disables PIM feature in the switch globally.
  - `ip pim component` - Configures the PIM component in the router.
  - `ip pim componentId` - Adds the interface to the PIM component.
  - `ip pim version` - Configures version number of the PIM protocol in the switch.
-

## 38.38 show ip pim thresholds

---

<b>Command Objective</b>	This command displays threshold configured for SPT, RP thresholds, and rate limit values for both SM (Sparse Mode).
<b>Syntax</b>	<code>show ip pim thresholds</code>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Note:</b>	This command executes only if PIM module is enabled globally.
<b>Example</b>	<pre>SEFOS# show ip pim thresholds PIM SPT Threshold Information   Group Threshold: 0   Source Threshold: 0   Switching Period: 0 PIM SPT-RP Threshold Information   Register Threshold: 0   RP Switching Period: 0   Register Stop rate limit: 5</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip pim/ ip multicast</code> - Enables or disables PIM feature in the switch globally.</li><li>• <code>set ip pim threshold</code> - Specifies the SPT group or source threshold. When the threshold exceeds, switching to shortest path tree is initiated.</li><li>• <code>set ip pim spt-switchperiod</code> - Specifies the period (in seconds) over which the data rate is to be monitored for switching to shortest path tree.</li><li>• <code>set ip pim rp-threshold</code> - Specifies the threshold at which the RP initiates switching to source specific shortest path tree.</li><li>• <code>set ip pim rp-switchperiod</code> - Specifies the period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree.</li><li>• <code>set ip pim regstop-ratelimit-period</code> - Specifies the period over which RP monitors number of register packets after sending the register stop message.</li></ul>

---

- 
- `set ip pim pmbr` – Enables or disables the PMBR (PIM Multicast Border Router) status.
  - `ip pim dr-priority` – Sets the designated router priority value configured for the router interface.
-



## 38.39 show ip pim mroute

<b>Command Objective</b>	This command displays the PIM multicast information. mroutes are multicast routing cache entries created by a user level mrouter daemon.
<b>Syntax</b>	<code>show ip pim mroute [bidir] [ {proxy   {compid(1-255)   group-address   source-address } summary } ]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>bidir</b> - Displays mroute with Bidir-PIM capable groups. Bidirectional PIM is an extension of PIM-SM, where multicast traffic can flow in both directions. All sources are potential receivers also.</li><li>• <b>proxy</b> - Displays RPF vector information.</li><li>• <b>Compid(1-255)</b> - Displays the component ID. This value ranges from 1 to 255.</li><li>• <b>group-address</b> - Displays the PIM multicast group address using the listed RP.</li><li>• <b>source-address</b> - Displays the network address which identifies the sources for which this entry contains multicast routing information.</li><li>• <b>summary</b> - Displays the summary of PIM mroute information.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Note:</b>	This command executes only if PIM module is enabled globally.
<b>Example</b>	<pre>SEFOS# show ip pim mroute IP Multicast Routing Table ----- Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit IIF State P: Pruned F: Forwarding A: Graft Ack Pending Timers: Uptime/Expires Interface State: Interface, State/Mode PIM Multicast Routing Table For Component 1 (12.0.0.10,227.1.1.1) ,00:00:03/05:43:11 Incoming Interface : vlan1 ,RPF nbr : NULL ,Route Flags : --- IIF State : P ,SRM Generation : Enabled</pre>

```

-----
Source Active Timer Value 210
Source Active Remaining Time : 05:43:11
State Refresh Remaining Time : 00:00:00
Prune Limit Remaining Time : 00:00:00
Outgoing Interface List : NULL

SEFOS# show ip pim mroute 1 summary
IP Multicast Routing Table
-----
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
Timers : Uptime/Expires
Interface State : Interface, State/Mode
PIM Multicast Routing Table For Component 1
(*, 224,1,0.0) , 00:04:35/--- , RP : 12.0.0.1
Incoming Interface : vlan1, RPF nbr : NULL, Route Flags :
WR
Outgoing InterfaceList:
  vlan2, Forwarding/Sparse, 00:04:35/---
(12.0.0.30,224.1.0.0) , 00:00:04/00:03:26
Incoming Interface : vlan1, RPF nbr : NULL, Route Flages :
S
Outgoing InterfaceList :
vlan2, Forwarding/Sparse , 00:00:04/---

SEFOS# show ip pim mroute bidir
IP Multicast Routing Table
-----
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
IIF State P: Pruned F: Forwarding A: Graft Ack Pending
Timers: Uptime/Expires
Interface State: Interface, State/Mode

```

---

**Related Command(s)**

- **ip pim component** - Configures the PIM component in the router.
  - **set ip pim/ ip multicast** - Enables or disables PIM feature in the switch globally.
  - **ip pim bsr-candidate - value** - Sets the preference value for the local interface as a candidate bootstrap router.
  - **ip pim bidir-enable** - Enables the Bidirectional PIM feature.
-

## 38.40 show ip pim redundancy state

---

<b>Command Objective</b>	This command displays the status of PIM HA feature (enabled or disabled), status of active and standby PIM instance, and status of dynamic bulk update.
--------------------------	---

---

<b>Syntax</b>	<code>show ip pim redundancy state</code>
---------------	---

---

<b>Mode</b>	Privileged EXEC Mode
-------------	----------------------

---

<b>Package</b>	Enterprise and Metro_E
----------------	------------------------

---

<b>Example</b>	<pre>SEFOS# show ip pim redundancy state Hot-standby feature is Enabled. Node State: Active,Standby Down. Dynamic Bulk Updates not started</pre>
----------------	--

---

## 38.41 show ip pim redundancy shadow-table

---

<b>Command Objective</b>	This command displays the shadow-table information for PIMv4 route entries.
<b>Syntax</b>	<code>show ip pim redundancy shadow-table</code>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Example</b>	<pre>SEFOS# show ip pim redundancy shadow-table Forwarding Plane Shadow Table : ----- (S, G) Incoming interface:( Alias / IfIndex) CPU Port Flag      :CPU Port Added / CPU Port Not Added Route Mode         : Sparse / Dense Route Status       : UnProcessed/Refreshed /New Outgoing InterfaceList :( Alias / IfIndex) (80.0.0.2, 224.6.6.6) Incoming interface:(vlan4 / 38) CPU Port Flag      :CPU Port Not Added Route Mode         :Dense Route Status       :New Outgoing InterfaceList :       (vlan2 / 36), (vlan14 / 34), (80.0.0.3, 224.6.6.6) Incoming interface:(vlan4 / 38) CPU Port Flag      :CPU Port Not Added Route Mode         :Dense Route Status       :New Outgoing InterfaceList :       (vlan2 / 36), (vlan14 / 34), Number of Entries : 2</pre>

---

## 38.42 ip pim bsr-border

---

**Command Objective** This command sets a PIM domain BSR (Bootstrap router) message border for an interface which stops the BSR message forwarding over the specified interface.

The no form of the command resets the PIM domain BSR message border.

---

**Syntax** `ip pim bsr-border`

`no ip pim bsr-border`

---

**Mode** Interface Configuration Mode (VLAN/Router)

---

**Package** Enterprise and Metro\_E

---

Note: This command is executed only if the PIM module is enabled.

---

**Example** `SEFOS (config-if) # ip pim bsr-border`

---

**Related Command(s)**

- `set ip pim` – Enables or disables the PIM globally.

---

## 38.43 set ip pim rpf vector

---

<b>Command Objective</b>	This command enables or disables the PIM RPF Vector TLV feature.
<b>Syntax</b>	<code>set ip pim rpf vector { enable   disable }</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>enable</code> - Enables RPF vector.</li><li>• <code>disable</code> - Disables RPF vector.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Note:</b>	This command is executed only if the PIM module is enabled.
<b>Example</b>	<code>SEFOS(config)# set ip pim rpf vector enable</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip pim/ ip multicast</code> - Enables or disables PIM feature in the switch globally.</li></ul>

---

## 38.44 ip pim bidir-enable

---

<b>Command Objective</b>	<p>This command enables the Bidirectional PIM feature.</p> <p>Bidirectional PIM is an extension of PIM-SM, where multicast traffic can flow in both directions. All sources are potential receivers also.</p> <p>The no form of the command disables the Bidirectional PIM feature.</p>
<b>Syntax</b>	<pre>ip pim bidir-enable</pre> <pre>no ip pim bidir-enable</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Example</b>	<pre>SEFOS(config)# ip pim bidir-enable</pre>
<u>Note:</u>	This command is executed only if the PIM module is enabled.
<b>Default</b>	Bidir PIM is disabled.
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip pim</code> – Enables or disables PIM globally.</li><li>• <code>rp-candidate rp-address</code> - Sets the address of the interface, which will be advertised as a Candidate-RP.</li><li>• <code>rp-static rp-address</code> - Sets the address of the interface, which will be advertised as a Static-RP.</li><li>• <code>ip pim bidir-offer-interval</code> – Configures the Bidir-PIM offer interval.</li><li>• <code>ip pim bidir-offer-limit</code> – Configures the Bidir-PIM offer limit.</li><li>• <code>show ip pim interface</code> - Displays the router's PIM interfaces.</li><li>• <code>show ip pim mroute</code> - Displays the PIM multicast information.</li><li>• <code>show ip pim rp-static</code> - Displays the static RP information.</li><li>• <code>show ip pim rp-set</code> - Displays the RP-set information.</li><li>• <code>show ip pim rp-candidate</code> - Displays the candidate RP information.</li></ul>

---

- 
- **show ip pim rp-hash** - Displays the elected RP for the multicast group address with the mask length.
  - **show ip pim interface df** - Displays the df states of all the PIM interfaces.
-



## 38.45 ip pim bidir-offer-interval

---

**Command Objective** This command configures the Bidir-PIM offer interval in milliseconds. It is the time interval between the Distance Forwarder (DF) election offer messages to be sent. This value ranges from 1 to 20000000 milliseconds.

The no form of the command resets the PIM Bidir-PIM offer interval to the default value.

---

**Syntax** `ip pim bidir-offer-interval <offer-interval> msec`  
`no ip pim bidir-offer-interval`

---

**Mode** Global Configuration Mode

---

**Package** Enterprise and Metro\_E

---

**Default** Offer-interval - 100 milliseconds

---

Note: This command executes only if,

- PIM module is enabled globally.
- Bidirectional PIM feature is enabled.

---

**Example** `SEFOS (config)# ip pim bidir-offer-interval 5000 msec`

---

**Related Command(s)**

- `set ip pim` – Enables or disables PIM globally.
- `ip pim bidir-enable` – Enables bidirectional PIM feature.
- `show ip pim interface detail` - Displays the PIMv6 interfaces of the router.

---

## 38.46 ip pim bidir-offer-limit

---

**Command Objective** This command configures the Bidir-PIM offer limit, the number of unanswered offers before the router changes to the designated forwarder (DF). This value ranges from 3 to 100.

The no command sets the Bidir-PIM offer-limit to the default value.

---

**Syntax** `ip pim bidir-offer-limit <offer-limit-integer>`  
`no ip pim bidir-offer-limit`

---

**Mode** Global Configuration Mode

---

**Package** Enterprise and Metro\_E

---

**Default** Offer-limit - 3

---

Note: This command executes only if,

- PIM module is enabled globally.
- Bidirectional PIM feature is enabled.

---

**Example** `SEFOS(config)# ip pim bidir-offer-limit 50`

---

**Related Command(s)**

- `set ip pim` – Enables or disables PIM globally.
- `ip pim bidir-enable` – Enables bidirectional PIM feature.
- `show ip pim interface detail` - Displays the PIMv6 interfaces of the router.

---

## 38.47 show ip pim rp-hash

---

<b>Command Objective</b>	This command displays the elected RP for the multicast group address with the mask length.
<b>Syntax</b>	<code>show ip pim rp-hash [&lt;multicast_Group_address&gt; &lt;Group_mask&gt;]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>&lt;multicast_Group_address&gt;</code> - Specifies the IP multicast group address for which this entry contains multicast routing information.</li><li>• <code>&lt;Group_Mask&gt;</code> - Specifies the IP multicast group address mask that gives the group prefix for which this entry contains information about the RP.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Example</b>	<pre>SEFOS# show ip pim rp-hash Component 1 ----- Group Address/Network Mask: 224.1.0.0/255.255.0.0 RP Address: 20.0.0.0 Priority: 192, Hold Time: 0</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip pim</code> – Enables or disables PIM globally.</li><li>• <code>ip pim bidir-enable</code> – Enables bidirectional PIM feature.</li><li>• <code>rp-candidate rp-address</code> – Sets the address of the interface, which will be advertised as a Candidate-RP.</li><li>• <code>ip pim bsr-candidate</code> - Sets the preference value for the local PIM interface as a candidate bootstrap router.</li><li>• <code>rp-candidate holdtime</code> - Configures the holdtime of the component when it is a candidate RP in the local domain.</li></ul>

---

## 38.48 ip pim external border

---

**Command Objective** This command sets an external non-PIM domain BSR message border for an interface which stops the BSR message forwarding over the specified interface.

The no form of the command resets the external non-PIM domain BSR message border.

---

**Syntax** `ip pim external border`

`no ip pim external border`

---

**Mode** Interface Configuration Mode (VLAN/Router)

---

**Package** Enterprise and Metro\_E

---

Note:

- This command is executed only if the PIM module is enabled.
- External border bit can be set only if,
  - Router is PMBR.
  - Admin status of the L3 interface is down.

---

**Example** `SEFOS(config-if)# ip pim external border`

---

**Related Command(s)**

- `set ip pim` - Enables or disables the PIM globally.
- `set ip pim pmbr` - Enables or disables the PIM Multicast Border Router (PMBR) Status.

---

## 38.49 show ip pim interface df

---

**Command Objective** This command displays the df states of all the PIM interfaces.

---

**Syntax** `show ip pim interface df`

---

**Mode** Privileged EXEC Mode

---

**Package** Enterprise and Metro\_E

---

Note:

- This command executes only if,
    - PIM module is enabled globally.
    - PIM multicast is configured.
    - PIM version is configured.
    - Bidirectional PIM feature is enabled.
    - Static RP configuration status is enabled.
    - PIM component is configured.
    - Candidate Bootstrap Router is configured.
    - Candidate-RP is configured.
    - Static-RP is configured.
    - Component mode to sparse or dense is configured.
- 

**Example** SEFOS # `show ip pim interface df`

```
Interface      RP Address      DF Winner      State
Metric Metric Pref  Up Time
-----
vlan1
Slot0/2      12.0.0.1      20.0.0.2      Win      0
0            00:00:36
```

---

**Related Command(s)**

- `set ip pim / ip multicast` – Enables or disables the PIM globally.
  - `ip pim version` - Configures version number of the PIM protocol.
  - `ip pim bidir-enable` – Enables bidirectional PIM feature.
  - `set ip pim static-rp` – Enables or disables the Static RP configuration status.
  - `rp-static rp-address` - Sets the address of the interface, which will be advertised as a Static-RP.
  - `rp-candidate rp-address` – Enables the address of the interface,
-

---

which will be advertised as a Candidate-RP.

- `ip pim componentId` - Adds the interface to the PIM component.
  - `ip pim bsr-candidate - value` - Sets the preference value for the local interface as a candidate bootstrap router.
  - `ip pim bsr-candidate - VLAN` - Sets the local interface as a candidate bootstrap router.
  - `set mode` - Sets the component mode to sparse or dense.
-

## **CHAPTER 39**

# **PIMv6**

---

PIMv6 is a portable software implementation of the PIM (Sparse Mode and Dense Mode) specification for IPv6 networks. The Oracle PIMv6 provides support for inter-domain routing between domains using PIMv6-SM or PIMv6-DM. It also avoids the performance problems of earlier multicast routing protocols. This software provides multicast routing and forwarding capability to a router that runs the IPv6 protocol along with MLD (Multicast Listener Discovery). The Oracle PIMv6 routes multicast data packets independent of any unicast routing protocol.

## 39.1 set ipv6 pim

<b>Command Objective</b>	This command enables or disables PIMv6 feature in the switch globally.
<b>Syntax</b>	<code>set ipv6 pim { enable   disable }</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>enable</code> - Enables PIMv6 feature in the switch.</li><li>• <code>disable</code> - Disables PIMv6 feature in the switch.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	disable
<b>Note:</b>	IGMP proxy service must be disabled in the system, before enabling the PIM globally.
<b>Example</b>	<pre>SEFOS (config)# set ipv6 pim enable</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>no ip igmp proxy-service</code> - Disables IGMP proxy service in the system.</li><li>• <code>set ipv6 pim lan-prune-delay</code> - Enables or disables the LanPruneDelay bit configured for the router interface to advertise the LAN delay.</li><li>• <code>ipv6 pim lan-delay</code> - Configures the LanDelay configured for the router interface.</li><li>• <code>ipv6 pim override-interval</code> - Configures the override interval configured for router interface.</li><li>• <code>iv6p pim dr-priority</code> - Configures the designated router priority value configured for the router interface.</li><li>• <code>ipv6 pim componentId</code> - Adds the interface to the PIMv6 component.</li><li>• <code>ipv6 pim bsr-candidate</code> - Configures the local interface as a candidate Bootstrap Router.</li><li>• <code>ipv6 pim message-interval</code> - Configures the frequency at which PIMv6 Join or Prune messages are transmitted on the PIM interface.</li><li>• <code>ipv6 pim query-interval</code> - Configures the frequency at which</li></ul>



---

PIMv6 hello messages are transmitted on this interface.

- **ipv6 pim rp-static rp-address** - Configures the address of the interface, which will be advertised as a Static-RP.
- **ipv6 pim rp-candidate rp-address** - Configures the address of the interface, which will be advertised as a Candidate-RP.
- **set mode** - Sets the component mode to sparse or dense.
- **set ip pim source-active interval** - Configures the time duration for which the SRM control messages would be originated by the router after a data packet is received.
- **set ipv6 pim graft-retry interval** - Configures the time before which graft is retransmitted upon no receipt of Graft ACK.
- **ip pim state-refresh disable** - Disables the SRM processing and forwarding.
- **set ip pim state-refresh origination-interval** - Configures the interval between successive SRM (State Refresh Messages) control messages originated and sent out by the router.
- **set ip pim static-rp** - Enables or disables the Static RP configuration status.
- **ip pim component** - Configures the PIM component in the router and enters into PIM component mode.
- **set ip pim pmbr** - Enables or disables the PIM Multicast Border Router (PMBR) Status.
- **set ip pim regstop-ratelimit-period** - Configures the period over which RP monitors the number of register packets after sending the register stop message.
- **set ip pim rp-switchperiod** - Configures the time period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree.
- **set ip pim threshold** - Configures the (Shortest Path Tree) SPT group or source threshold.
- **set ip pim rp-threshold** - Configures the threshold at which the RP (Rendezvous Point) initiates switching to source specific shortest path tree.
- **set ip pim spt-switchperiod** - Configures the time period (in seconds) over which the data rate is to be monitored for switching to shortest path tree.
- **set ip pim threshold** - Configures the Shortest Path Tree (SPT)

---

group or source threshold.

- **debug ipv6 pim** - Enables the tracing of the PIM module as per the configured debug levels.
  - **ipv6 pim bsr-border** - Sets a PIMv6 domain BSR (Bootstrap router) message border for an interface.
  - **no ipv6 pim interface** - Deletes an interface at PIM level.
  - **ip pim bidir-enable**- Enables the Bidirectional PIM feature.
  - **ip pim bidir-offer-interval** – Configures the Bidir-PIM offer interval in milliseconds.
  - **ip pim bidir-offer-limit** – Configures the Bidir-PIM offer limit.
  - **show ipv6 pim mroute** - Displays the PIMv6 multicast information.
  - **show ipv6 pim thresholds** – Displays the threshold configured for SPT, RP thresholds, and rate limit values for both SM
  - **show ipv6 pim component** - Displays the component information. The component ID value ranges between 1 and 255.
  - **show ipv6 pim rp-static** - Displays the static RP information.
  - **show ipv6 pim bsr** - Displays the BSR information.
  - **show ipv6 pim rp-set** - Displays the RP-set information.
  - **show ipv6 pim rp-candidate** - Displays the candidate RP information.
  - **show ipv6 pim neighbor** - Displays the router's PIM neighbors' information.
  - **show ipv6 pim interface** - Displays the router's PIM interfaces.
  - **show ipv6 pim rp-hash** - Displays the elected RP for the multicast group address with the mask length.
-

## 39.2 set ip pim threshold

---

<b>Command Objective</b>	This command configures the SPT (Shortest Path Tree) group or source threshold which, when exceeded, leads to switching to shortest path tree based on number of bits per sec. To switch to SPT, the threshold must be configured.
<b>Syntax</b>	<code>set ip pim threshold { spt-grp   spt-src } &lt; number of packets (0-2147483647) &gt;</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>spt-grp</code> - Initiates the source specific counters when the threshold of data rate for any group exceeds. It is based on number of packets.</li><li>• <code>spt-src</code> - Initiates the switching to Shortest Path Tree when the threshold of data rate for any source exceeds. It is based on number of packets.</li><li>• <code>&lt;number of packets (0-2147483647)&gt;</code> - Sets the number of packets. This value ranges from 0 to 2147483647.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Note:</b>	This command executes only if PIM or PIMv6 module is enabled globally.
<b>Default</b>	0
<b>Example</b>	<code>SEFOS (config)# set ip pim threshold spt-grp 50</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ipv6 pim</code> - Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>set ip pim / ip multicast</code> - Enables or disables the PIM globally.</li><li>• <code>set ip pim spt-switchperiod</code> - Configures the time period (in seconds) over which the data rate is to be monitored for switching to shortest path tree.</li><li>• <code>show ipv6 pim thresholds</code> - Displays threshold configured for SPT, RP thresholds, and rate limit values for both SM and DM.</li></ul>

---

## 39.3 set ip pim spt-switchperiod

---

<b>Command Objective</b>	This command configures the period (in seconds) over which the data rate is to be monitored for switching to shortest path tree. The same period is used for monitoring the data rate for both source and group. To switch to SPT, this period must be configured. The SPT is used for multicast transmission of packets with the shortest path from sender to recipients.
<b>Syntax</b>	<code>set ip pim spt-switchperiod &lt;0-2147483647 (in secs)&gt;</code>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	0
<b>Note:</b>	This command executes only if the PIM or PIMv6 is enabled in the switch.
<b>Example</b>	<code>SEFOS (config)# set ip pim spt-switchperiod 60</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip pim / ip multicast</code> - Enables or disables the PIM globally.</li><li>• <code>set ipv6 pim</code> - Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>show ipv6 pim thresholds</code> - Displays threshold configured for SPT, RP thresholds, and rate limit values for both SM and DM.</li></ul>

---

## 39.4 set ip pim rp-threshold

---

**Command Objective** This command sets the threshold at which RP (Rendezvous Point) initiates switching to source-specific shortest path tree. The number of registered packets ranges between 0 and 2147483647.

To switch to SPT, this threshold must be configured. This switching is based on the received number of registered packets.

---

**Syntax** `set ip pim rp-threshold <0-2147483647(number of reg packets)>`

---

**Mode** Global Configuration Mode

---

**Package** Enterprise and Metro\_E

---

**Default** 0

---

Note: This command executes only if PIM or PIMv6 module is enabled globally.

---

**Example** `SEFOS (config)# set ip pim rp-threshold 50`

---

**Related Command(s)**

- `set ipv6 pim` - Enables or disables PIMv6 feature in the switch globally.
- `set ip pim / ip multicast` - Enables or disables the PIM globally.
- `show ipv6 pim thresholds` - Displays threshold configured for SPT, RP thresholds, and rate limit values for both SM and DM.

---

## 39.5 set ip pim rp-switchperiod

---

<b>Command Objective</b>	<p>This command sets the period (in seconds) over which RP monitors register packets for switching to the source-specific shortest path tree. This value ranges from 0 to 2147483647.</p> <p>To switch to SPT, this period must be configured. RP-tree is a pattern that multicast packets are sent to a PIM-SM router by unicast and then forwarded to actual recipients from RP.</p>
<b>Syntax</b>	<code>set ip pim rp-switchperiod &lt;0-2147483647(in secs)&gt;</code>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	0
<b>Note:</b>	This command executes only if PIM or PIMv6 module is enabled globally.
<b>Example</b>	<pre>SEFOS (config)# set ip pim rp-switchperiod 100</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ipv6 pim</code> - Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>set ip pim / ip multicast</code> - Enables or disables the PIM globally.</li><li>• <code>show ipv6 pim thresholds</code> - Displays threshold configured for SPT, RP thresholds, and rate limit values for both SM and DM.</li></ul>

---

## 39.6 set ip pim regstop-ratelimit-period

---

**Command Objective** This command sets the period over which RP monitors the number of register packets after sending the register stop message. This value ranges from 0 to 2147483647.

The Register Stop Message is used to avoid encapsulation of multicast data packets from the first hop router to the RP.

---

**Syntax** `set ip pim regstop-ratelimit-period <0-2147483647 (in secs)>`

---

**Mode** Global Configuration Mode

---

**Package** Enterprise and Metro\_E

---

**Default** 5

---

Note: This command executes only if PIM or PIMv6 module is enabled globally.

---

**Example** `SEFOS (config)# set ip pim regstop-ratelimit-period 100`

---

**Related Command(s)**

- `set ipv6 pim` - Enables or disables PIMv6 feature in the switch globally.
- `set ip pim / ip multicast` - Enables or disables the PIM globally.
- `show ipv6 pim thresholds` - Displays threshold configured for SPT, RP thresholds, and rate limit values for both SM and DM.

---

## 39.7 set ip pim pmbr

---

<b>Command Objective</b>	This command enables or disables the PMBR (PIM Multicast Border Router) status.  A PMBR integrates two different PIM domains (either PIM-SM or PIM-DM) and also connects a PIM domain to other multicast routing domain(s).
<b>Syntax</b>	<code>set ip pim pmbr { enable   disable }</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>enable</code> - Enables the PMBR status.</li><li>• <code>disable</code> - Disables the PMBR status.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	Disable
	<u>Note:</u> This command executes only if PIM or PIMv6 module is enabled globally.
<b>Example</b>	<code>SEFOS (config)# set ip pim pmbr enable</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ipv6 pim</code> - Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>set ip pim / ip multicast</code> - Enables or disables the PIM globally.</li><li>• <code>show ipv6 pim thresholds</code> - Displays threshold configured for SPT, RP thresholds, and rate limit values for both SM.</li></ul>

---



## 39.8 set ip pim static-rp

---

<b>Command Objective</b>	This command enables or disables the Static RP configuration status. This command specifies whether to use the configured static RP.
<b>Syntax</b>	<code>set ip pim static-rp { enable   disable }</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>enable</code> - Enables the Static RP configuration status.</li><li>• <code>disable</code> - Disables the Static RP configuration status.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	disable
<b>Note:</b>	This command executes only if PIM or PIMv6 module is enabled globally.
<b>Example</b>	<code>SEFOS (config)# set ip pim static-rp enable</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ipv6 pim</code> - Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>set ip pim / ip multicast</code> - Enables or disables the PIM globally.</li><li>• <code>show ipv6 pim rp-set</code> - Displays the RP-set information.</li><li>• <code>show ipv6 pim rp-static</code> - Displays the RP-static information.</li></ul>

---

## 39.9 ip pim component

---

**Command Objective** This command configures the PIMv6 component in the router and enters into PIM component mode. The PIMv6 component corresponds to each instance of a PIMv6 domain and classifies it as Sparse or Dense mode.

The no form of the command destroys the PIMv6 component. This value ranges from 2 to 255.

The PIMv6 Component 1 cannot be deleted as it is the default component.

---

**Syntax** `ip pim component <ComponentId (1-255)> [Scope-zone-name (64) ]`

`no ip pim component <ComponentId (2-255)>`

---

**Parameter Description**

- `<ComponentId (1-255)>` - Configures the PIM component in the router and enters into PIM component mode. This value ranges from 1 to 255.
- `Scope-zone-name (64)` - Configures the scope-zone name. The maximum length of the string is 64. To configure the scope-zone name, scope-zone should be created in the interface. Scope is a 4-bit value that describes the scope of an IPv6 address. A unicast address can possibly have 2 scopes (Linklocal and Global) only and a multicast address can have a maximum of 11 scopes. The scope zone name should be the same as that of the zone created in the `ipv6 scope-zone` command. If `ipv6 scope-zone` is created as `scopeA 1`, then the scope-zone name should be `scopeA1` (without whitespace).

---

**Mode** Global Configuration Mode

---

**Package** Enterprise and Metro\_E

---

**Default** Component-Id - 1

---

Note: This command executes only if PIM or PIMv6 module is enabled globally.

---

**Example**

```
SEFOS (config)# ip pim component 1
SEFOS (pim-comp)#
```

---

**Related Command(s)**

- `set ip pim / ip multicast` - Enables or disables the PIM globally.
- `set ipv6 pim` - Enables or disables PIMv6 feature in the switch globally.
- `ipv6 scope-zone` - Creates IPv6 scope zone on an interface.

---

- 
- `show ipv6 pim component` - Displays the component information.
-

## 39.10 ipv6 pim rp-candidate rp-address

---

<b>Command Objective</b>	<p>This command sets the address of the interface, which is advertised as a Candidate-RP.</p> <p>A Candidate-RP is a router configured to send periodic Candidate-RP-Advertisement messages to the BSR. A Candidate-RP processes Join, Prune, or Register messages for the advertised group prefix, when it is elected as a RP.</p> <p>The no form of the command disables the address of the interface, which is advertised as a Candidate-RP.</p>
<b>Syntax</b>	<pre>ipv6 pim rp-candidate rp-address &lt;Group Address&gt; &lt;Group Mask&gt; &lt;RP-address&gt; [Priority 0-255] [bidir]</pre> <pre>no ipv6 pim rp-candidate rp-address &lt;Group Address&gt; &lt;Group Mask&gt; &lt;RP address&gt; [Priority 0-255]</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>&lt;Group Address&gt;</b> - Configures the IPv6 multicast group address for which the local router advertises itself as a Candidate-RP.</li><li>• <b>&lt;Group Mask&gt;</b> - Configures the IPv6 multicast group address mask that gives the group prefix for which the entry contains information about Candidate-RP.</li><li>• <b>&lt;RP address&gt;</b> - Configures the IPv6 address of the candidate Rendezvous Point.</li><li>• <b>Priority &lt;0-255&gt;</b> - Sets the priority of the Candidate-RP. This value ranges from 0 to 255.</li><li>• <b>bidir</b> - Configures bidirectional status of RP. Bidirectional PIM is an extension of PIM-SM, where multicast traffic can flow in both directions. All sources are potential receivers also.</li></ul>
<b>Mode</b>	PIM Component Mode
<b>Package</b>	Enterprise and Metro_E
<b>Note:</b>	<p>This command executes only if,</p> <ul style="list-style-type: none"><li>• PIM module is enabled globally.</li><li>• PIM mode is set as sparse.</li><li>• PIM query interval and IPv6 address is configured.</li></ul>

---

- 
- Bidirectional PIM should be enabled to use the bidir option.
- 

**Example**

```
SEFOS(pim-comp)# ipv6 pim rp-candidate rp-address  
ff02::e001:0000 112 3333::1111
```

---

**Related Command(s)**

- `set ipv6 pim` - Enables or disables PIMv6 feature in the switch globally.
  - `ip pim component` - Configures the PIM component in the router.
  - `ip pim bidir-enable` – Enables bidirectional PIM feature.
  - `ipv6 address` - Sets the IPv6 address for an interface.
  - `ipv6 pim componentId` - Adds the interface to the PIMv6 component.
  - `show ipv6 pim rp-set` – Displays the PIMv6 RP-set information.
  - `show ipv6 pim rp-candidate` – Displays the PIMv6 RP-candidate information.
  - `show ipv6 pim rp-hash` - Displays the elected RP for the multicast group address with the mask length.
-

## 39.11 ipv6 pim rp-static rp-address

---

<b>Command Objective</b>	<p>This command sets the address of the IPv6 interface, which will be advertised as a Static-RP.</p> <p>The Static configuration allows additional structuring of the multicast traffic by directing the multicast join or prune messages to statically configured RPs.</p> <p>The no form of the command disables the address of the IPv6 interface, which will be advertised as a Static-RP.</p>
<b>Syntax</b>	<pre>ipv6 pim rp-static rp-address &lt;Group Address&gt; &lt;Group Mask&gt; &lt;RP address&gt; [bidir]  no ipv6 pim rp-static rp-address &lt;Group Address&gt; &lt;Group Mask&gt;</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>&lt;Group Address&gt;</b> - Configures the PIMv6 Sparse multicast group address using the listed RP.</li><li>• <b>&lt;Group Mask&gt;</b> - Configures the IPv6 multicast group address mask that gives the group prefix for which this entry contains information about RP.</li><li>• <b>&lt;RP address&gt;</b> - Configures the IPv6 address of the static Rendezvous Point.</li><li>• <b>bidir</b> - Configures the bidirectional status of the RP. Bidirectional PIM is an extension of PIM-SM, where multicast traffic can flow in both directions. All sources are potential receivers also.</li></ul>
<b>Mode</b>	PIM Component Mode
<b>Package</b>	Enterprise and Metro_E
<b>Note:</b>	<p>This command executes only if,</p> <ul style="list-style-type: none"><li>• PIM module is enabled globally.</li><li>• PIM mode is set as sparse.</li><li>• Bidirectional PIM should be enabled to use the bidir option.</li></ul>
<b>Example</b>	<pre>SEFOS (pim-comp) # ipv6 pim rp-static rp-address ff02::e001:0000 112 3333::1111 bidir</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>set ipv6 pim</b> - Enables or disables PIMv6 feature in the switch globally.</li></ul>

---

- 
- `ip pim component` - Configures the PIM component in the router.
  - `ip pim bidir-enable` – Enables bidirectional PIM feature.
  - `ipv6 pim componentId` - Configures the PIM component in the router.
  - `ip pim Component` – Enters the PIM component mode.
  - `show ipv6 pim rp-static` – Displays the RP-static information.
  - `show ipv6 pim rp-hash` - Displays the elected RP for the multicast group address with the mask length.
-

## 39.12 ipv6 pim query-interval

---

<b>Command Objective</b>	<p>This command sets the frequency at which PIMv6 hello messages are transmitted on the interface. The interval ranges between 0 and 65535.</p> <p>The query message informs the neighboring routers of the presence of a PIMv6 router on the interface.</p> <p>The no form of the command sets the default hello timer interval for the interface.</p>
<b>Syntax</b>	<pre>ipv6 pim query-interval &lt;Interval (0-65535) secs&gt;</pre> <pre>no ipv6 pim query-interval</pre>
<b>Mode</b>	Interface Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	30
	<p><u>Note:</u> This command executes only if the PIMv6 module is enabled globally in the switch.</p>
<b>Example</b>	<pre>SEFOS (config-if)# ipv6 pim query-interval 60</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ipv6 pim</code> - Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>show ipv6 pim interface</code> – Displays the PIMv6 interfaces of the router.</li></ul>

---



## 39.13 ipv6 pim message-interval

---

**Command Objective** This command sets the frequency at which the PIMv6 Join or Prune messages are transmitted on the PIMv6 interface. The interval ranges between 0 and 65535.

The Join or Prune message interval used on all the PIMv6 routers in the PIMv6 domain must be the same. If all the routers do not use the same timer interval, the performance of PIMv6 Sparse can be adversely affected.

The no form of the command sets the default value for the PIMv6 Join or Prune messages.

---

**Syntax** `ipv6 pim message-interval <Interval(0-65535)>`  
`no ipv6 pim message-interval`

---

**Mode** Interface Configuration Mode

---

**Package** Enterprise and Metro\_E

---

**Default** 60

---

Note: This command executes only if the PIMv6 module is enabled globally in the switch.

---

**Example** `SEFOS (config-if)# ipv6 pim message-interval 120`

---

**Related Command(s)**

- `set ipv6 pim` - Enables or disables PIMv6 feature in the switch globally.
- `show ipv6 pim interface` – Displays the PIMv6 interfaces of the router.

---

## 39.14 ipv6 pim bsr-candidate

---

**Command Objective** This command configures the preference value for the local PIMv6 interface as a candidate bootstrap router. This value ranges from 0 to 255. A BSR is a dynamically elected router within the PIMv6 domain.

The no form of the command sets the default preference value for the local PIMv6 interface as a candidate bootstrap router.

---

**Syntax** `ipv6 pim bsr-candidate <value (0-255)>`  
`no ipv6 pim bsr-candidate`

---

**Mode** Interface Configuration Mode

---

**Package** Enterprise and Metro\_E

---

**Default** 0

---

Note: This command executes only if the PIMv6 module is enabled globally in the switch.

---

**Example** `SEFOS (config-if)# ipv6 pim bsr-candidate 1`

---

**Related Command(s)**

- `set ipv6 pim` - Enables or disables PIMv6 feature in the switch globally.
- `ipv6 pim rp-candidate rp-address` - Sets the address of the interface, which will be advertised as a Candidate-RP.
- `show ipv6 pim bsr` - Displays the PIMv6 BSR information.

---

## 39.15 ipv6 pim componentId

---

**Command Objective** This command adds the interface to the PIMv6 component. The component ID ranges between 1 and 255. This command adds the current VLAN into the specified PIMv6 component.

The no form of the command removes the interface from the PIMv6 component.

---

**Syntax**

```
ipv6 pim componentId <value(1-255)>

no ipv6 pim componentId <value(1-255)>
```

---

**Mode** Interface Configuration Mode (VLAN/Router)

---

**Package** Enterprise and Metro\_E

---

**Default** 1

---

Note: This command executes only if the PIMv6 module is enabled globally in the switch.

---

**Example**

**Interface Configuration Mode (VLAN)**

```
SEFOS(config)# interface vlan 3
SEFOS (config-if)# ipv6 pim componentId 1
```

**Interface Configuration Mode (Router)**

```
SEFOS(config)# interface extreme-ethernet 0/2
SEFOS(config-if)# no switchport
SEFOS (config-if)# ipv6 pim componentId 1
```

---

**Related Command(s)**

- **set ipv6 pim** – Enables or disables PIMv6 feature in the switch globally.
- **ip pim component** – Configures the PIM component in the router and enters into PIM component mode.
- **ipv6 pim rp-candidate rp-address** - Sets the address of the interface, which will be advertised as a Candidate-RP.
- **ipv6 pim rp-static rp-address** – Sets the address of the interface, which will be advertised as a Static-RP.

---

- 
- `show ipv6 pim interface` – Displays the routers PIMv6 interfaces.
  - `show ipv6 pim component` – Displays the component information.
  - `set ipv6 pim graft-retry interval` – Configures the time before which graft is retransmitted upon no receipt of Graft ACK.
-

## 39.16 ipv6 pim hello-holdtime

---

<b>Command Objective</b>	<p>This command sets the holdtime for the hello message for the PIMv6 interface. The holdtime value ranges between 1 and 65535. Holdtime is the amount of time, in seconds, a receiver must keep the neighbor reachable.</p> <p>The no form of the command sets the default holdtime for the hello message for the interface.</p>
	<hr/> <p>This command is obsolete.</p> <hr/>
<b>Syntax</b>	<pre>ipv6 pim hello-holdtime &lt;holdtime (1-65535)&gt;  no ipv6 pim hello-holdtime</pre> <hr/>
<b>Mode</b>	Interface Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	105
<b>Example</b>	<pre>SEFOS (config-if)# ipv6 pim hello-holdtime 180</pre> <hr/>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ipv6 pim neighbor</code> – Displays the PIMv6 neighbor(s) information of the router.</li></ul> <hr/>

## 39.17 ipv6 pim dr-priority

---

**Command Objective** This command configures the designated router priority value configured for the PIMv6 router interface. The priority value ranges between 1 and 4294967295.

The DR sets up multicast route entries and sends corresponding Join, Prune, and Register messages on behalf of directly-connected receivers and sources, respectively.

The no form of the command resets the designated router priority value for the PIMv6 router interface to its default value.

---

**Syntax** `ipv6 pim dr-priority <priority>`

`no ipv6 pim dr-priority`

---

**Mode** Interface Configuration Mode (VLAN/Router)

---

**Package** Enterprise and Metro\_E

---

**Default** 1

---

Note: This command executes only if the PIMv6 module is enabled globally in the switch.

---

**Example** `SEFOS (config-if)# ipv6 pim dr-priority 100`

---

**Related Command(s)**

- `set ipv6 pim` – Enables or disables PIMv6 feature in the switch globally.
- `show ipv6 pim interface` – Displays the PIMv6 interfaces of the router.

---

## 39.18 ipv6 pim override-interval

---

<b>Command Objective</b>	<p>This command sets the override interval configured for the PIMv6 router interface. The override interval ranges between 0 and 65535.</p> <p>The override interval is the random amount of time delay for sending override messages. The purpose of the override interval is to avoid synchronization of override messages when multiple downstream routers share a multi-access link.</p> <p>The no form of the command sets the default override interval for the PIMv6 router interface.</p>
<b>Syntax</b>	<pre>ipv6 pim override-interval &lt;interval (0-65535)&gt;  no ipv6 pim override-interval</pre>
<b>Mode</b>	Interface Configuration Mode (VLAN)
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	0
	<p><u>Note:</u> This command executes only if the PIMv6 module is enabled globally in the switch.</p>
<b>Example</b>	<pre>SEFOS (config-if)# ipv6 pim override-interval 100</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ipv6 pim</code> – Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>show ipv6 pim interface</code> – Displays the PIMv6 interfaces of the router.</li></ul>

---

## 39.19 ipv6 pim lan-delay

---

**Command Objective** This command sets the LanDelay configured for the PIMv6 router interface. The LAN delay value ranges between 0 and 65535.

The LAN Delay inserted by a router in the LAN Prune Delay option performs the expected message propagation delay on the interface. It is used by upstream routers to find out the delayed time interval for a Join override message before pruning an interface.

The no form of the command sets the default LanDelay for the PIMv6 router per interface.

---

**Syntax** `ipv6 pim lan-delay <value(0-65535)>`

`no ipv6 pim lan-delay`

---

**Mode** Interface Configuration Mode (VLAN)

---

**Package** Enterprise and Metro\_E

---

**Default** 0

---

Note: This command executes only if the PIMv6 module is enabled globally in the switch.

---

**Example** `SEFOS (config-if)# ipv6 pim lan-delay 120`

---

**Related Command(s)**

- `set ipv6 pim` – Enables or disables PIMv6 feature in the switch globally.
- `show ipv6 pim interface` – Displays the PIMv6 interfaces of the router.

---



## 39.20 set ipv6 pim lan-prune-delay

---

<b>Command Objective</b>	This command enables or disables the LanPruneDelay bit configured for the PIMv6 router interface to advertise the LAN delay. The command specifies whether to use LAN prune delay or not.
<b>Syntax</b>	<code>set ipv6 pim lan-prune-delay { enable   disable }</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• enable - Enables LAN prune delay</li><li>• disable - Disables LAN prune delay</li></ul>
<b>Mode</b>	Interface Configuration Mode (VLAN)
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	disable
<b>Note:</b>	This command executes only if the PIMv6 module is enabled globally in the switch.
<b>Example</b>	<code>SEFOS (config-if)# set ipv6 pim lan-prune-delay enable</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ipv6 pim</code> – Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>show ipv6 pim interface</code> – Displays the PIMv6 interfaces of the router.</li></ul>

---

## 39.21 set ipv6 pim graft-retry interval

---

**Command Objective** This command configures the time before which graft is retransmitted upon no receipt of Graft ACK. This value ranges from 1 to 10.

The no form of the command sets the graft retry interval to its default value.

---

**Syntax** `set ipv6 pim graft-retry interval <value(1-10)>`  
`no ipv6 pim graft-retry interval`

---

**Mode** Interface Configuration Mode (VLAN /Router)

---

**Package** Enterprise and Metro\_E

---

**Default** 3 seconds

---

Note: This command executes only if PIMv6 module is enabled globally.

To configure the graft-retry interval, the PIMv6 component that the interface is mapped to should be in dense mode.

---

**Example** **Interface Configuration Mode (VLAN)**

```
SEFOS(config)# interface vlan 3
SEFOS(config-if)# set ipv6 pim graft-retry interval 4
```

**Interface Configuration Mode (Router)**

```
SEFOS(config)# interface extreme-ethernet 0/2
SEFOS(config-if)# no switchport
SEFOS(config-if)# set ipv6 pim graft-retry interval 4
```

---

**Related Command(s)**

- `set ip pim/ ip multicast` - Enables or disables PIM feature in the switch globally.
- `set mode` - Sets the component mode to sparse or dense.
- `ipv6 pim componentId` - Adds the interface to the PIMv6 component.
- `show ipv6 pim interface detail` - Displays the router's PIMv6 interfaces.

---

## 39.22 no ipv6 pim interface

---

<b>Command Objective</b>	This command deletes the IPv6 PIM interface. It is used to destroy the interface at PIMv6.
<b>Syntax</b>	<code>no ipv6 pim interface</code>
<b>Mode</b>	Interface Configuration Mode (VLAN)
<b>Package</b>	Enterprise and Metro_E
<u>Note:</u>	This command executes only if the PIMv6 module is enabled globally in the switch.
<b>Example</b>	<code>SEFOS (config-if)# no ipv6 pim interface</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ipv6 pim</code> – Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>show ipv6 pim interface</code> – Displays the PIMv6 interfaces of the router.</li></ul>

---

## 39.23 debug ipv6 pim

---

**Command Objective** This command enables the tracing of the PIMv6 module as per the configured debug levels. The trace statements are generated for the configured trace levels.

This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

The no form of the command disables the tracing of the PIMv6 module as per the configured debug levels. The trace statements are not generated for the configured trace levels.

---

**Syntax**

```
debug ipv6 pim
{ [nbr] [grp] [jp] [ast] [bsr] [io] [pmbr] [mrt] [mdh] [mgmt] [srm]
[red] | [all] }

no debug ipv6 pim
{ [nbr] [grp] [jp] [ast] [bsr] [io] [pmbr] [mrt] [mdh] [mgmt] [srm]
[red] | [all] }
```

---

**Parameter Description**

- **nbr** - Sets the module as PIM Neighbor Discovery module, for which the tracing is to be done as per the configured debug levels.
  - **grp** - Generates debug statements for group membership traces.
  - **jp** - Generates debug statements for Join or Prune traces.
  - **ast** - Generates debug statements for assert state traces.
  - **bsr** - Generates debug statements for Bootstrap or RP traces.
  - **io** - Generates debug statements for input and output traces.
  - **pmbr** - Generates debug statements for interoperability traces.
  - **mrt** - Generates debug statements for Multicast Route Table Update traces.
  - **mdh** - Generates debug statements for Multicast Data Handling traces.
  - **mgmt** - Generates debug statements for management traces.
  - **srm** - Generates debug statements for state refresh messages.
  - **red** - Sets the module as PIM redundancy module, for which the tracing is to be done as per the configured debug levels.
-

---

	<ul style="list-style-type: none"> <li>• <code>all</code> - Generates debug statements for all kinds of traces.</li> </ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
	<p><u>Note:</u> This command executes only if the PIMv6 module is enabled globally in the switch.</p>
<b>Example</b>	<code>SEFOS # debug ipv6 pim all</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"> <li>• <code>set ipv6 pim</code> – Enables or disables PIMv6 feature in the switch globally.</li> <li>• <code>show ipv6 pim interface</code>– Displays the PIMv6 interfaces of the router.</li> </ul>

---

## 39.24 show ipv6 pim interface

---

**Command Objective** This command displays the PIMv6 interface details of the router. The details include the list of interface addresses, the mode of the interface, Designated Router on that interface, Hello Interval, and Join or Prune Interval of the interface.

---

**Syntax** `show ipv6 pim interface [{ Vlan <vlan-id/vfi-id> [df] | detail }]`

---

**Parameter Description**

- **Vlan <vlan-id/vfi-id>** - Displays PIMv6 interface details for the specified VLAN / VFI ID. This value ranges from 1 to 65535.
  - **<vlan -id>** - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.
  - **<vfi-id>** - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.

---

**Note:** The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.

**Note:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.

**Note:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.

---

- **df** - Displays the Bidir-PIM Designated Forwarder (DF) related information.
- **detail** - Displays the detailed information of the IPv6 PIM interface.

---

**Mode** Privileged EXEC Mode

---

**Package** Enterprise and Metro\_E

---

**Note:** This command executes only if the PIMv6 module is enabled globally in the switch.

---

**Example**

```
SEFOS# show ipv6 pim interface
Address      IfName/      Ver/      Nbr      Qry      DR      DR
              IfId         Mode     Count Interval Address
```

---

```

-----
Prio-
-----
-
fe80::2:a00:1 vlan1/33  2/Sparse  0   150  fe80::2:a00:1
1
fe80::2:1400:1 vlan2/34  2/Sparse  0   30  fe80::2:1400:1
1
fe80::2:1e00:1 vlan3/35  2/Sparse  0   30  fe80::2:1e00:1
1

```

**SEFOS# show ipv6 pim interface vlan 1**

```

Address      IfName/      Ver/      Nbr      Qry      DR      DR
              IfId         Mode      Count  Interval  Address Prio-
-----
--
fe80::2:a00:1 vlan1/33  2/Sparse  0   150  fe80::2:a00:1
1

```

**SEFOS# show ipv6 pim interface detail**

```

vlan1 73 is up
  Internet Address is fe80::202:2ff:fe03:401
  Multicast Switching : Enabled
  PIM : Enabled
  PIMv6 : Enabled
    PIM version : 2, mode: Sparse
    PIM DR : fe80::202:2ff:fe03:401
    PIM DR Priority : 1
    PIM Neighbour Count : 0
    PIM Hello/Query Interval : 30
    PIM Message Interval : 60
    PIM Override Interval : 0
    PIM Lan Delay : 0
    PIM Lan-Prune-Delay : Disabled
    PIM Component Id : 1
    PIM domain border : disabled
    PIM RPF Status : Disabled
    PIM Bidirectional Status : Enabled
      Offer Interval : 5000, Offer Limit : 100

```

**SEFOS# show ipv6 pim interface vlan 2 df**

```

RP Address      DF Winner      State  Metric Metric Pref
-----

```

---

```
3333::1111      ::      Lose      -1      2147483647
```

---

**Related Command(s)**

- **set ipv6 pim** – Enables or disables PIMv6 feature in the switch globally.
  - **ip pim componentId** - Adds the interface to the PIM component.
  - **ip pim component** - Configures the PIM component in the router.
  - **ip pim version** - Configures version number of the PIM protocol in the switch.
  - **ip pim bidir-enable**- Enables the Bidirectional PIM feature.
  - **ipv6 pim query-interval** – Sets the frequency at which PIMv6 hello messages are transmitted on the interface.
  - **ipv6 pim message-interval** – Sets the frequency at which PIMv6 Join or Prune messages are transmitted on the PIMv6 interface.
  - **ipv6 pim bsr-candidate** – Sets the preference value for the local PIMv6 interface as a candidate bootstrap router.
  - **ipv6 pim dr-priority** – Sets the designated router priority value configured for the PIMv6 router interface.
  - **ipv6 pim override-interval** – Sets the override interval configured for the PIMv6 router interface.
  - **ipv6 pim lan-delay** – Sets the LanDelay configured for the PIMv6 router interface.
  - **set ipv6 pim lan-prune-delay** – Sets the LanPruneDelay bit configured for the PIMv6 router interface to advertise the LAN delay.
  - **set ipv6 pim graft-retry interval** - Configures the time before which graft is retransmitted upon no receipt of Graft ACK.
  - **no ipv6 pim interface** – Deletes an interface at PIMv6 level.
  - **debug ipv6 pim** – Enables PIMv6 trace.
  - **ipv6 pim rp-candidate rp-address** - Sets the address of the interface, which will be advertised as a Candidate-RP.
  - **ip pim bidir-offer-interval** – Configures the Bidir-PIM offer interval in milliseconds.
  - **ip pim bidir-offer-limit** – Configures the Bidir-PIM offer limit.
-



## 39.25 show ipv6 pim neighbor

---

**Command Objective** This command displays the PIMv6 neighbor(s) information of the router. The information contains the neighbor address, the interface used to reach the PIMv6 neighbor, the up time (the time since this neighbor became the neighbor of the local router), expiry time (the minimum time remaining before this PIMv6 neighbor will be aged out), and LAN delay and override interval.

---

**Syntax** `show ipv6 pim neighbor [Vlan <vlan-id/vfi-id>]`

---

**Parameter Description**

- **Vlan <vlan-id/vfi-id>** - Displays PIMv6 interface details for the specified VLAN / VFI ID. This value ranges from 1 to 65535.
  - **<vlan -id>** - VLAN ID is a unique value that represents the specific VLAN. This value ranges from 1 to 4094.
  - **<vfi-id>** - VFI ID is a VLAN created in the system which contains pseudowires and attachment circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges from 4096 to 65535.

---

**Note:** The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or filtering database entries.

**Note:** VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.

**Note:** The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to hundred added to the maximum number of VLANs. An error message is displayed for any value beyond this range.

---

**Mode** Privileged EXEC Mode

---

**Package** Enterprise and Metro\_E

---

**Note:** This command executes only if the PIMv6 module is enabled globally in the switch.

---

**Example**

**SEFOS# show ipv6 pim neighbor**

Nbr Lan	If Name	Uptime/ Expiry	Ver	DRPri/ Mode	Comp Id	Over- ride
Address Delay						

/Idx

---

```

-----
Interval
-----
--
fe80::2:a00:a  vlan1/33  00:02:33/0    v2  0/S    1    0
0
fe80::2:1400:a  vlan2/34  00:02:33/0    v2  0/S    1    0
0

SEFOS# show ipv6 pim neighbor vlan 1

Nbr      If      Uptime/      Ver  DRPri/  Comp Over-
Lan
Address  Name    Expiry      Mode  Id  ride
Delay
/Idx
Interval
-----
--
fe80::2:a00:a  vlan1/33  00:02:58/0    v2  0/S    1    0
0

```

**Related Command(s)**

- **set ipv6 pim** – Enables or disables PIMv6 feature in the switch globally.
- **ip pim component** - Configures the PIM component in the router.
- **ipv6 pim componentId** - Adds the interface to the PIMv6 component.
- **ipv6 pim query-interval** – Sets the frequency at which PIMv6 hello messages are transmitted on the interface.
- **ipv6 pim message-interval** – Sets the frequency at which PIMv6 Join or Prune messages are transmitted on the PIMv6 interface.
- **ipv6 pim bsr-candidate** – Sets the preference value for the local PIMv6 interface as a candidate bootstrap router.
- **ipv6 pim hello-holdtime** – Sets the holdtime for the hello message for the PIMv6 interface.

## 39.26 show ipv6 pim rp-candidate

---

<b>Command Objective</b>	This command displays the PIMv6 RP-candidate information. The information contain group addresses, group mask, and RP address that indicates the IP address of the Rendezvous Point (RP) for the listed PIM Sparse group.
<b>Syntax</b>	<code>show ipv6 pim rp-candidate [ComponentId &lt;1-255&gt;] [bidir]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>ComponentId &lt;1-255&gt;</code> - Displays the specified component ID for candidate RP information. This value ranges from 1 to 255.</li><li>• <code>bidir</code> - Displays the Bidir-PIM capable groups. Bidirectional PIM is an extension of PIM-SM, where multicast traffic can flow in both directions. All sources are potential receivers also.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Note:</b>	This command executes only if the PIMv6 module is enabled globally in the switch.
<b>Example</b>	<pre>SEFOS# show ipv6 pim rp-candidate 1 bidir CompId      GroupAddress/PrefixLength      RPAddress/Priority ----- 1           ff02::e000:0/112                3333::a00:1/192</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ipv6 pim</code> - Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>ip pim component</code> - Configures the PIM component in the router.</li><li>• <code>ipv6 pim componentId</code> - Adds the interface to the PIMv6 component.</li><li>• <code>ip pim bidir-enable</code> - Enables the Bidirectional PIM feature.</li><li>• <code>ipv6 pim bsr-candidate</code> - Sets the preference value for the local PIMv6 interface as a candidate bootstrap router.</li><li>• <code>ipv6 pim rp-candidate rp-address</code> - Sets the address of the interface, which will be advertised as a Candidate-RP.</li><li>• <code>ipv6 pim rp-static rp-address</code> - Sets the address of the interface, which will be advertised as a Static-RP.</li><li>• <code>show ipv6 pim rp-hash</code> - Displays the elected RP for the multicast group address with the mask length.</li></ul>

---

## 39.27 show ipv6 pim rp-set

<b>Command Objective</b>	This command displays the PIMv6 RP-set information. The details include group prefix, RP address, hold time and expiry time.
<b>Syntax</b>	<code>show ipv6 pim rp-set [rp-address]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>rp-address</code> - Displays the IPv6 address of the Rendezvous Point (RP) for the listed PIM Sparse group.</li><li>• <code>bidir</code> - Displays Bidir-PIM capable groups. Bidirectional PIM is an extension of PIM-SM, where multicast traffic can flow in both directions. All sources are potential receivers also.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Note:</b>	This command executes only if the PIMv6 module is enabled globally in the switch.
<b>Example</b>	<pre>SEFOS# show ipv6 pim rp-set 3333::a00:a bidir PIM Group-to-RP mappings ----- Group Address : ff00::Group Mask : 8 RP: 3333::a00:a Component-Id : 1 Hold Time : 102, Expiry Time : 00:00:35</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ipv6 pim</code> – Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>ipv6 pim rp-candidate rp-address</code> – Enables the address of the interface, which will be advertised as a Candidate-RP.</li><li>• <code>ipv6 pim rp-static rp-address</code> – Sets the address of the interface, which will be advertised as a Static-RP.</li><li>• <code>ip pim component</code> - Configures the PIM component in the router.</li><li>• <code>ipv6 pim componentId</code> - Adds the interface to the PIMv6 component.</li><li>• <code>ip pim bidir-enable</code>- Enables the Bidirectional PIM feature.</li><li>• <code>ipv6 pim bsr-candidate</code> – Sets the preference value for the local PIMv6 interface as a candidate bootstrap router.</li></ul>

- 
- `ipv6 pim rp-candidate rp-address` – Enables the address of the interface, which will be advertised as a Candidate-RP.
  - `ipv6 pim rp-static rp-address` – Sets the address of the interface, which will be advertised as a Static-RP.
  - `set ip pim static-rp` – Enables or disables the Static RP configuration status.
  - `rp-candidate holdtime` – Sets the hold time of the component when it is a candidate RP in the local domain.
  - `show ipv6 pim rp-hash` - Displays the elected RP for the multicast group address with the mask length.
-

## 39.28 show ipv6 pim bsr

---

<b>Command Objective</b>	This command displays the PIMv6 BSR information. The component ID ranges between 1 and 255.
<b>Syntax</b>	<code>show ipv6 pim bsr [Component-Id (1-255)]</code>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<u>Note:</u>	This command executes only if the PIMv6 module is enabled globally in the switch.
<b>Example</b>	<pre>SEFOS# show ipv6 pim bsr 1 PIMv2 Bootstrap Configuration For Component 1 ----- Elected BSR for Component 1 V6 BSR Address : 3333::a00:1 V6 BSR Priority : 100, Hash Mask Length : 126 This System is V6 Candidate BSR for Component 1 V6 BSR Address : 3333::a00:1 V6 BSR Priority : 100</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ipv6 pim</code> – Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>ip pim component</code> - Configures the PIM component in the router.</li><li>• <code>ipv6 pim componentId</code> - Adds the interface to the PIMv6 component.</li><li>• <code>ipv6 pim bsr-candidate</code> – Sets the preference value for the local interface as a candidate bootstrap router.</li></ul>

---

## 39.29 show ipv6 pim rp-static

---

<b>Command Objective</b>	This command displays the static RP information.
<b>Syntax</b>	<code>show ipv6 pim rp-static [ComponentId &lt;1-255&gt;] [bidir]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>ComponentId &lt;1-255&gt;</b> - Specifies the component ID for which the static RP information is to be displayed. This value ranges from 1 to 255.</li><li>• <b>bidir</b> - Displays the Bidir-PIM capable groups. Bidirectional PIM is an extension of PIM-SM, where multicast traffic can flow in both directions. All sources are potential receivers also.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Note:</b>	This command executes only if the PIMv6 module is enabled globally in the switch.
<b>Example</b>	<pre>SEFOS# show ipv6 pim rp-static bidir Static-RP Enabled CompId   GroupAddress/PrefixLength   RPAddress Embedded ----- --           1   ff70:340:3333::1/128       3333::3   Enabled</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>set ipv6 pim enable</b> - Enables or disables PIMv6 feature in the switch globally.</li><li>• <b>ipv6 pim rp-static rp-address</b> - Enables or disables the Static RP configuration status.</li><li>• <b>ip pim component</b> - Configures the PIM component in the router.</li><li>• <b>ipv6 pim componentId</b> - Adds the interface to the PIMv6 component.</li><li>• <b>shutdown - physical/VLAN/port-channel/tunnel interface</b> - Disables a physical interface, VLAN interface, port-channel interface, tunnel interface, or OOB interface.</li><li>• <b>ipv6 interface-identifier</b> - Configures 64 bit IPv6 interface identifier on the interface.</li><li>• <b>ipv6 address</b> - Configures IPv6 address on the interface.</li></ul>

---

- 
- `ipv6 nd prefix` - Configures the prefix to be advertised in IPv6 Router Advertisement.
  - `ip pim bidir-enable` - Enables Bidirectional PIM.
  - `embedded-rp` - Configures the address of the IPv6 interface, which is advertised as an Embedded RP.
  - `set ip pim static-rp` - Enables or disables the Static RP configuration status.
  - `show ipv6 pim rp-hash` - Displays the elected RP for the multicast group address with the mask length.
-



## 39.30 show ipv6 pim component

---

<b>Command Objective</b>	This command displays the PIM component information. The information contains the component ID, PIM mode, version, BSR, and RP hold time. The component ID ranges between 1 and 255.
<b>Syntax</b>	<code>show ipv6 pim component [ComponentId &lt;1-255&gt;]</code>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<u>Note:</u>	This command executes only if the PIMv6 module is enabled globally in the switch.
<b>Example</b>	<pre>SEFOS# show ipv6 pim component 1 PIM Component Information ----- Component-Id: 1   PIM Mode: sparse,   PIM Version: 2   Elected BSR: 10.0.0.1   Candidate RP Holdtime: 0</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ipv6 pim</code> – Enables or disables PIMv6 feature in the switch globally.</li><li>• <code>ip pim component</code> - Configures the PIM component in the router.</li><li>• <code>ipv6 pim componentId</code> – Adds the interface to the PIMv6 component.</li><li>• <code>ip pim version</code> - Configures version number of the PIM protocol in the switch.</li></ul>

---

## 39.31 show ipv6 pim thresholds

---

<b>Command Objective</b>	This command displays threshold configured for SPT, RP thresholds, and rate limit values for both SM and DM.
<b>Syntax</b>	<b>show ipv6 pim thresholds</b>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<u>Note:</u>	This command executes only if the PIMv6 module is enabled globally in the switch.
<b>Example</b>	<pre>SEFOS# show ipv6 pim thresholds PIM SPT Threshold Information ----- Group Threshold   : 111 Source Threshold  : 222 Switching Period  : 100 PIM SPT-RP Threshold Information ----- Register Threshold       : 333 RP Switching Period     : 300 Register Stop rate limit : 400</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>set ipv6 pim</b> – Enables or disables PIMv6 feature in the switch globally.</li><li>• <b>set ip pim threshold</b> – Configures the SPT group or source threshold.</li><li>• <b>set ip pim spt-switchperiod</b> – Configures the period (in seconds) over which the data rate is to be monitored for switching to shortest path tree.</li><li>• <b>set ip pim rp-threshold</b> – Sets the threshold at which the RP initiates switching to source specific shortest path tree.</li><li>• <b>set ip pim rp-switchperiod</b> – Sets the period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree.</li><li>• <b>set ip pim regstop-ratelimit-period</b> – Sets the period over which RP monitors number of register packets after sending the register</li></ul>

---

---

stop message.

- **set ip pim pmbr**— Enables or disables the PMBR (PIM Multicast Border Router) status.
  - **ipv6 pim dr-priority**— Sets the designated router priority value configured for the router interface.
-

## 39.32 show ipv6 pim mroute

---

<b>Command Objective</b>	This command displays the IPv6 PIM mroute information.  mroutes are multicast routing cache entries created by a user level mrouting daemon.
<b>Syntax</b>	<pre>show ipv6 pim mroute [bidir] [ {proxy   {compid(1-255)   group &lt;group-address&gt;   source &lt;source-address&gt; } summary } ]</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>bidir</b> - Displays mroute with Bidir-PIM capable groups. Bidirectional PIM is an extension of PIM-SM, where multicast traffic can flow in both directions. All sources are potential receivers also.</li><li>• <b>proxy</b> - Displays the proxy details.</li><li>• <b>compid(1-255)</b> - Displays the component ID.</li><li>• <b>group &lt;group-address&gt;</b> - Displays the PIMv6 multicast group address using the listed RP.</li><li>• <b>source &lt;source-address&gt;</b> - Displays the network address which identifies the sources for which the entry contains multicast routing information.</li><li>• <b>summary</b> - Displays the summary of PIMv6 mroute information.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Note:</b>	This command executes only if the PIMv6 module is enabled globally in the switch.
<b>Example</b>	<pre>SEFOS# show ipv6 pim mroute IP Multicast Routing Table ----- Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit Timers: Uptime/Expires Interface State: Interface, State/Mode PIM Multicast Routing Table For Component 1 (*, ff02::e001:0) ,00:03:54/---3401:510a::3401:51a) Incoming Interface : vlan1</pre>

---

---

```
,RPF nbr : fe80::2:a00:a ,Route Flags : WR
Outgoing InterfaceList :
vlan2, Forwarding/Sparse ,00:03:54/---
```

```
SEFOS# show ipv6 pim mroute group ff02::e001:0 summary
```

```
IP Multicast Routing Table
```

```
-----
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
```

```
Timers: Uptime/Expires
```

```
PIM Multicast Routing Table For Component 1
```

```
(*, ff02::e001:0) ,00:02:49/---3401:510a::3401:51a) ,Route
Flags : WR
```

```
SEFOS# show ipv6 pim mroute source ca8d:5102::ca8d:5102
summary
```

```
IP Multicast Routing Table
```

```
-----
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
```

```
Timers: Uptime/Expires
```

```
(ca8d:5102::ca8d:5102,ff02::e001:0) ,00:01:04/04:01:45
,Route Flags : ---
```

```
SEFOS# show ipv6 pim mroute bidir
```

```
IP Multicast Routing Table
```

```
-----
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
```

```
IIF State P: Pruned F: Forwarding A: Graft Ack Pending
```

```
Timers: Uptime/Expires
```

```
Interface State: Interface, State/Mode
```

---

**Related Command(s)**

- **set ipv6 pim** – Enables or disables PIMv6 feature in the switch globally.
  - **ipv6 pim bsr-candidate** – Sets the preference value for the local IPv6 interface as a candidate bootstrap router.
  - **ip pim bidir-enable** – Enables the Bidirectional PIM feature.
-

## 39.33 show ip pim redundancy state

---

<b>Command Objective</b>	This command displays the status of PIM HA feature (enabled or disabled), status of active and standby PIM instance, and status of dynamic bulk update.
<b>Syntax</b>	<code>show ip pim redundancy state</code>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Example</b>	<pre>SEFOS# show ip pim redundancy state Hot-standby feature is Enabled. Node State: Active,Standby Down. Dynamic Bulk Updates not started</pre>

---

## 39.34 show ipv6 pim redundancy shadow-table

---

<b>Command Objective</b>	This command displays the shadow-table information for PIMv6 route entries.
<b>Syntax</b>	<code>show ipv6 pim redundancy shadow-table</code>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Example</b>	<pre>SEFOS# show ipv6 pim redundancy shadow-table Forwarding Plane Shadow Table : ----- (S, G) Incoming interface:( Alias / IfIndex) CPU Port Flag      :CPU Port Added / CPU Port Not Added Route Mode         : Sparse / Dense Route Status       : UnProcessed/Refreshed /New Outgoing InterfaceList :( Alias / IfIndex) (8080::5000:2, ff01::e006:606) Incoming interface:(vlan4 / 36) CPU Port Flag      :CPU Port Not Added Route Mode         :Dense Route Status       :New Outgoing InterfaceList :       (vlan14 / 38), (vlan2 / 34), (8080::5000:3, ff01::e006:606) Incoming interface:(vlan4 / 36) CPU Port Flag      :CPU Port Not Added Route Mode         :Dense Route Status       :New Outgoing InterfaceList :       (vlan14 / 38), (vlan2 / 34), Number of Entries : 2</pre>

---

## 39.35 ipv6 pim bsr-border

---

**Command Objective** This command sets a PIMv6 domain BSR (Bootstrap Router) message border for an interface which stops the BSR message forwarding over the specified interface.

The no form of the command resets the PIMv6 domain BSR message border.

---

**Syntax** `ipv6 pim bsr-border`  
`no ipv6 pim bsr-border`

---

**Mode** Interface Configuration Mode (VLAN/Router)

---

**Package** Enterprise and Metro\_E

---

Note: This command is executed only if the PIMv6 module is enabled.

---

**Example** `SEFOS(config-if)# ip pim bsr-border`

---

**Related Command(s)**

- `set ipv6 pim` – Enables or disables the PIMv6 module globally.

---



## 39.36 embedded-rp

---

<b>Command Objective</b>	<p>This command configures the address of the IPv6 interface, which is advertised as an Embedded RP (Rendezvous point).</p> <p>The no form of the command disables the advertisement of the listed IPv6 interface address as Embedded-RP address.</p>
<b>Syntax</b>	<pre>embedded-rp &lt;RP Address&gt; &lt;Group Address&gt; &lt;Group-address-prefix-length&gt;</pre> <pre>no embedded-rp &lt;Group Address&gt; &lt;Group-address-prefix-length&gt;</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• &lt;RP Address&gt; - Configures IPv6 address of the rendezvous point.</li><li>• &lt;Group Address&gt; - Configures PIMv6 sparse multicast group address using the listed RP.</li><li>• &lt;Group-address-prefix-length&gt; - Configures the prefix length. This value ranges from 97 to 128.</li></ul>
<b>Mode</b>	PIM Component Mode
<b>Default</b>	The address of the IPv6 interface which is advertised as an Embedded-RP is disabled
<b>Package</b>	Enterprise and Metro_E
<b>Note:</b>	<p>This command executes if,</p> <ul style="list-style-type: none"><li>• PIM and PIMv6 modules are enabled globally in the switch.</li><li>• IPv6 module is enabled.</li><li>• IPv6 interface identifier, IPv6 prefix, and IPv6 address are configured on an interface.</li><li>• Static RP configuration status is enabled.</li><li>• The interface is shut down.</li></ul>
<b>Example</b>	<pre>SEFOS (pim-comp)# embedded-rp 33::34 ff7e:3440:33::15 128</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ipv6 pim rp-static</code> - Displays the static RP information.</li><li>• <code>shutdown - physical/VLAN/port-channel/tunnel interface</code> - Disables a physical interface, VLAN interface, port-channel interface,</li></ul>

---

---

tunnel interface, or OOB interface.

- **ipv6 enable** - Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
  - **ipv6 interface-identifier** - Configures 64 bit IPv6 interface identifier on the interface.
  - **ipv6 address** - Configures IPv6 address on the interface.
  - **ipv6 nd prefix** - Configures the prefix to be advertised in IPv6 Router Advertisement.
  - **set ip pim** – Enables or disables the PIM globally.
  - **set ipv6 pim** – Enables or disables the PIMv6 module globally.
  - **set ip pim static-rp enable** - Enables or disables the Static RP configuration status.
  - **ipv6 pim componentId** – Adds the interface to the component.
  - **ip pim component** - Configures the PIM component in the router.
-

## 39.37 ip pim bidir-enable

---

<b>Command Objective</b>	<p>This command enables the Bidirectional PIM feature.</p> <p>Bidirectional PIM is an extension of PIM-SM, where multicast traffic can flow in both directions. All sources are potential receivers also.</p> <p>The no form of the command disables the Bidirectional PIM feature.</p>
<b>Syntax</b>	<pre>ip pim bidir-enable</pre> <pre>no ip pim bidir-enable</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Example</b>	<pre>SEFOS(config)# ip pim bidir-enable</pre>
<b>Note:</b>	This command is executed only if the PIM module is enabled.
<b>Default</b>	Bidir PIM is disabled
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip pim</code> – Enables or disables PIM globally.</li><li>• <code>rp-candidate rp-address</code> - Sets the address of the interface, which will be advertised as a Candidate-RP.</li><li>• <code>rp-static rp-address</code> - Sets the address of the interface, which will be advertised as a Static-RP.</li><li>• <code>ip pim bidir-offer-interval</code> – Configures the Bidir-PIM offer interval.</li><li>• <code>ip pim bidir-offer-limit</code> – Configures the Bidir-PIM offer limit.</li><li>• <code>show ip pim interface</code> - Displays the router's PIM interfaces.</li><li>• <code>show ip pim mroute</code> - Displays the PIM multicast information.</li><li>• <code>show ip pim rp-static</code> - Displays the static RP information.</li><li>• <code>show ip pim rp-set</code> - Displays the RP-set information.</li><li>• <code>show ip pim rp-candidate</code> - Displays the candidate RP information.</li></ul>

---

- 
- **show ip pim rp-hash** - Displays the elected RP for the multicast group address with the mask length.
-

## 39.38 ip pim bidir-offer-interval

---

**Command Objective** This command configures the Bidir-PIM offer interval in milliseconds. It is the time interval between the Designated Forwarder (DF) election offer messages to be sent. This value ranges from 1 to 20000000 milliseconds.

The no form of the command resets the PIM Bidir-PIM offer interval to the default value.

---

**Syntax** `ip pim bidir-offer-interval <offer-interval> msec`

`no ip pim bidir-offer-interval`

---

**Mode** Global Configuration Mode

---

**Package** Enterprise and Metro\_E

---

**Default** Offer-interval - 100 milliseconds

---

Note: This command executes only if,

- PIM module is enabled globally.
- Bidirectional PIM feature is enabled.

---

**Example** `SEFOS(config)# ip pim bidir-offer-interval 5000 msec`

---

**Related Command(s)**

- `set ip pim` – Enables or disables PIM globally.
- `ip pim bidir-enable` – Enables bidirectional PIM feature.
- `show ip pim interface detail` - Displays the PIMv6 interfaces of the router.

---

## 39.39 ip pim bidir-offer-limit

---

**Command Objective** This command configures the Bidir-PIM offer limit, the number of unanswered offers before the router changes as the designated forwarder (DF). It is the number of unanswered offers to change the state as DF winner. This value ranges from 3 to 100.

The no command sets the Bidir-PIM offer limit to the default value.

---

**Syntax** `ip pim bidir-offer-limit <offer-limit-integer>`

`no ip pim bidir-offer-limit`

---

**Mode** Global Configuration Mode

---

**Package** Enterprise and Metro\_E

---

**Default** Offer-limit - 3

---

Note: This command executes only if,

- PIM module is enabled globally.
- Bidirectional PIM feature is enabled.

---

**Example** `SEFOS(config)# ip pim bidir-offer-limit 50`

---

**Related Command(s)**

- `set ip pim` – Enables or disables PIM globally.
- `ip pim bidir-enable` – Enables bidirectional PIM feature.
- `show ip pim interface detail` - Displays the PIMv6 interfaces of the router.

---

## 39.40 show ipv6 pim rp-hash

---

<b>Command Objective</b>	This command displays the elected RP for the multicast group address with the mask length.
<b>Syntax</b>	<code>show ipv6 pim rp-hash [&lt;multicast Group address&gt; &lt;Group Mask-Length&gt;]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <code>&lt;multicast_Group_address&gt;</code> - Displays the IPv6 multicast group address for which this entry contains multicast routing information.</li><li>• <code>&lt;Group_Mask-Length&gt;</code> - Displays the IPv6 multicast group address mask that gives the group prefix for which the entry contains information about RP. This value ranges from 0 to 128.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Metro_E and Enterprise
<b>Example</b>	<pre>SEFOS# show ipv6 pim rp-hash Component 1 ----- Group Address/Mask Length: ff02::e001:0/112 RP Address 3333::1111 Priority: 192, Hold Time: 100</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ipv6 pim</code> – Enables or disables PIM globally.</li><li>• <code>ip pim bidir-enable</code> – Enables bidirectional PIM feature.</li><li>• <code>ipv6 pim componentId</code> – Adds the interface to the PIM component.</li><li>• <code>ipv6 pim bsr-candidate</code> – Sets the preference value for the local PIM interface as a candidate bootstrap router.</li><li>• <code>ipv6 pim rp-candidate rp-address</code> – Sets the address of the interface, which will be advertised as a Candidate-RP.</li><li>• <code>rp-candidate holdtime</code> – Sets the hold time of the component when it is a candidate RP in the local domain.</li><li>• <code>ipv6 pim bsr-candidate</code> – Sets the preference value for the local PIMv6 interface as a candidate bootstrap router.</li></ul>

---





# IPv4 Multicasting

---

IPv4 is a connectionless protocol for use on packet-switched Link Layer networks, operating on a best effort delivery model.

IP multicasting is the sending of a single datagram to multiple hosts on a network or inter-network. Of the three delivery methods supported by IP, multicasting is the method that is most practical for one-to-many delivery. Unlike IP multicasting, IP unicasting sends a separate datagram to each recipient host. IP broadcasting sends a single datagram to all hosts on a single network segment (also known as subnet), even to those not interested in receiving it. Recent trends toward multimedia applications such as video conferencing necessitate the use of multicasting to efficiently send traffic to multiple hosts.

The list of CLI commands for the configuration of IPv4 multicasting is as follows:

- [ip multicast routing](#)
- [ip multicast-routing](#)
- [ip mcast ttl-threshold](#)
- [ip mcast rate-limit](#)
- [show ip mroute](#)

---

Note: These commands are available only when NPAPI is enabled. IPv4 Multicasting commands cannot be executed in Linux Simulation environment or NP Simulator environment.

---

## 40.1 ip multicast routing

<b>Command Objective</b>	This command enables the forwarding of IP multicast packets.  The no form of the command disables the forwarding of IP multicast packets.
	This command is available only when NPAPI is enabled.
<b>Syntax</b>	<code>ip multicast routing</code>  <code>no ip multicast routing</code>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	IP multicast routing is enabled.
<b>Example</b>	<code>SEFOS(config)# ip multicast routing</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip mroute</code> - Displays the multicast route information.</li></ul>

## 40.2 ip multicast-routing

---

<b>Command Objective</b>	<p>This command enables the forwarding of IP multicast packets.</p> <p>The no form of the command disables the forwarding of IP multicast packets.</p> <p>This command is a standardized implementation of the existing command <code>ip multicast routing</code>. Its operation is similar to the existing command.</p>
	<hr/> <p>This command is available only when NPAPI is disabled.</p> <hr/>
<b>Syntax</b>	<pre>ip multicast-routing</pre> <pre>no ip multicast-routing</pre> <hr/>
<b>Mode</b>	Global Configuration Mode <hr/>
<b>Package</b>	Enterprise and Metro_E <hr/>
<b>Default</b>	IP multicast routing is enabled. <hr/>
<b>Example</b>	<pre>SEFOS(config)# ip multicast-routing</pre> <hr/>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>show ip mroute</code> - Displays the multicast route information.</li></ul> <hr/>

## 40.3 ip mcast ttl-threshold

<b>Command Objective</b>	<p>This command configures the TTL (time-to-live) threshold for multicast router interface.</p> <p>The no form of the command removes the TTL threshold for multicast router interface.</p>
	<p>This command is available only when NPAPI is enabled.</p>
<b>Syntax</b>	<pre>ip mcast ttl-threshold &lt;ttl-threshold (0-255)&gt;  no ip mcast ttl-threshold</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• &lt;ttl-threshold (0-255)&gt; - Configures the datagram TTL threshold for the interface. This value ranges from 0 to 255. Any IP multicast datagrams with a TTL less than this threshold will not be forwarded out of the interface. The TTL threshold value of 0 means all the multicast packets are forwarded out of the interface.</li></ul>
<b>Mode</b>	Interface Configuration Mode (VLAN)
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	ttl-threshold - 0
	<p><u>Note:</u></p> <ul style="list-style-type: none"><li>• This command executes only if DVMRP is enabled on the specific interface.</li><li>• PIM and IGMP Proxy also need to be enabled for the command functionality.</li></ul>
<b>Example</b>	<pre>SEFOS(config)# set ip dvmrp enable  SEFOS (config)# interface vlan 2  SEFOS (config-if)# set ip dvmrp enable  SEFOS (config-if)# ip mcast ttl-threshold 45</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>set ip dvmrp enable</code> - Enables DVMRP in the switch or on a specific interface.</li><li>• <code>set ip pim enable</code> - Enables PIM feature in the switch.</li><li>• <code>ip igmp proxy-service</code> - Enables IGMP proxy service functionality in the system and starts protocol operations.</li></ul>

- 
- `show ip mroute` - Displays the multicast route information.
-

## 40.4 ip mcast rate-limit

<b>Command Objective</b>	<p>This command configures the rate limit value (in Kbit/sec) for multicast router interface.</p> <p>The no form of the command disables rate limiting on the multicast router interface.</p>
	<p>This command is available only when NPAPI is enabled.</p>
<b>Syntax</b>	<pre>ip mcast rate-limit &lt;rate-limit (kbps)&gt;  no ip mcast rate-limit</pre>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>&lt;rate-limit (kbps)&gt;</b> - Configures the rate limit value, in kilobits per second, of forwarded multicast traffic on the interface. A rate limit of 0 indicates that no rate limiting is done.</li></ul>
<b>Mode</b>	Interface Configuration Mode (VLAN)
<b>Package</b>	Enterprise and Metro_E
<b>Default</b>	0
	<p><u>Note:</u></p> <ul style="list-style-type: none"><li>• This command executes only if DVMRP is enabled on the specific interface.</li><li>• PIM and IGMP Proxy also need to be enabled for the command functionality.</li></ul>
<b>Example</b>	<pre>SEFOS(config-if)# ip mcast rate-limit 0</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>set ip dvmrp enable</b> - Enables DVMRP in the switch or on a specific interface.</li><li>• <b>set ip pim enable</b> - Enables PIM feature in the switch.</li><li>• <b>ip igmp proxy-service</b> - Enables IGMP proxy service functionality in the system and starts protocol operations.</li><li>• <b>show ip mroute</b> - Displays the multicast route information.</li></ul>

## 40.5 show ip mroute

<b>Command Objective</b>	This command displays the multicast route information. <hr/> This command is available only when NPAPI is enabled.
<b>Syntax</b>	<code>show ip mroute</code>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Enterprise and Metro_E
<b>Example</b>	<pre>SEFOS# show ip mroute IPv4 Multicast Routing Status : Enabled Multicast Routing Information ----- (S,G), uptime/expires Muticast routing protocol, Upstream neighbor Incoming interface : interface Outgoing interface list :     interface, state, uptime/expires (20.0.0.10, 224.1.0.0), 0d 00:00:13.83/ 0d 00:01:30.23 PIM-SM, 0.0.0.0 Incoming interface: vlan 2 Outgoing interface list:     vlan 1, Forwarding, 0d 00:00:13.82/0d 00:01:30.22</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ip multicast-routing/ ip multicast-routing</code> – Enables the forwarding of IP multicast packets.</li><li>• <code>ip mcast ttl-threshold</code> - Sets the TTL (time-to-live) threshold for multicast router interface.</li><li>• <code>ip mcast rate-limit</code> - Sets the rate limit value (in Kbit/sec) for multicast router interface.</li></ul>





## CHAPTER 41

# TAC

---

Transmission and admission control (TAC) is a utility module that is used by multicast protocols for filtering multicast packets and multicast VLAN classification. The profile table and filter table present in the TAC module are built through administrator configuration. All configured addresses are stored as address ranges. When a report is received on a particular interface, the corresponding profile mapped to this interface is obtained and filter rule table is scanned to determine if a match exists for the address present in the incoming report. If the address is present in the profile with permission as `permit`, the reports are processed, else they are dropped.

---

**Note:** BCM Chipset porting is not done for this module.

---

## 41.1 ip mcast profile

---

**Command Objective** This command creates or modifies a multicast profile and enters profile configuration mode. The profile, once created, will have the permission details configured. The client's source address is maintained in the entry with the permission type as allow or deny. The reports from the client are processed by matching it with the profile ID.

The no form of this command deletes a multicast profile.

---

**Syntax**

```
ip mcast profile <profile-id> [description (128)]  
  
no ip mcast profile <profile-id>
```

---

**Parameter Description**

- **<profile-id>** - Configures the profile identifier for the multicast profile entry. This value ranges from 1 to 4294967295.
- **description (128)** - Configures the description for the clients' details.

---

**Mode** Global Configuration Mode

---

**Package** Workgroup and Metro\_E

---

Note: This command can be executed only if the profile ID is not configured for multicast VLAN classification and the multicast profile index is not configured for a downstream interface.

---

**Example** SEFOS(config)# ip mcast profile 1 sample

---

**Related Command(s)**

- **no ip igmp snooping multicast-vlan profile** – Removes the profile ID-to-VLAN mapping for multicast VLAN classification.
- **ip igmp snooping ratelimit** – Configures the rate limit for a downstream interface in units of the number of IGMP packets per second.
- **ip igmp snooping limit** – Configures the maximum limit type for an interface.
- **ip igmp snooping filter-profileId** – Configures the multicast profile index for a downstream interface.
- **no ip igmp snooping filter-profileId** – Resets the multicast profile index to default value.
- **permit** – Configures the action for the profile as permit.
- **deny** – Configures the action for the profile as deny.

---

- 
- **range** – Creates or modifies a filter.
  - **profile active** – Activates the profile entry.
  - **show ip mcast profile** – Displays the filters configured in the profile and the profile statistics.
-

## 41.2 ip igmp profile

---

<b>Command Objective</b>	<p>This command creates or modifies a multicast profile and enters profile configuration mode. This value ranges from 1 to 4294967295.</p> <p>The no form of the command deletes a multicast profile.</p> <p>This command is a standardized implementation of the existing command <code>ip mcast profile</code>. Its operation is similar to the existing command.</p>
<b>Syntax</b>	<pre>ip igmp profile &lt;profile-id&gt;</pre> <pre>no ip igmp profile &lt;profile-id&gt;</pre>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup and Metro_E
<b>Note:</b>	This command can be executed only if the profile ID is not configured for multicast VLAN classification and the multicast profile index is not configured for a downstream interface.
<b>Example</b>	<pre>SEFOS(config)# ip igmp profile 1</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>no ip igmp snooping multicast-vlan profile</code> – Removes the profile ID-to-VLAN mapping for multicast VLAN classification.</li><li>• <code>ip igmp snooping ratelimit</code> – Configures the rate limit for a downstream interface in units of the number of IGMP packets per second.</li><li>• <code>ip igmp snooping limit</code> – Configures the maximum limit type for an interface.</li><li>• <code>permit</code> - Configures the action for the profile as permit.</li><li>• <code>deny</code> – Configures the action for the profile as deny.</li><li>• <code>range</code> – Creates or modifies a filter.</li><li>• <code>profile active</code> – Activates the profile entry.</li><li>• <code>show ip mcast profile</code> – Displays the filters configured in the profile and the profile statistics.</li></ul>

---

## 41.3 set ip mcast profiling

---

<b>Command Objective</b>	This command enables or disables IGMP profiling in the switch.
<b>Syntax</b>	<code>set ip mcast profiling {enable/disable}</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>enable</b> - Configures the profiling to be enabled. When enabled, the profile is allowed to be created.</li><li>• <b>disable</b> - Configures the profiling to be disabled. New profiles are not allowed to be created.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup and Metro_E
<b>Default</b>	Profiling is enabled.
<b>Example</b>	<code>SEFOS(config)# set ip mcast profiling enable</code>

---

## 41.4 permit

---

<b>Command Objective</b>	This command configures the action for the channels associated with this profile as permit. When the profile action is permit, the matching rule is executed. The IGMPv3 reports with specific source list is modified with the sources that are permitted and the denied sources are removed from the list.
<b>Syntax</b>	<code>permit</code>
<b>Mode</b>	Profile Configuration Mode
<b>Package</b>	Workgroup and Metro_E
<b>Default</b>	Profile action is deny.
<b>Note:</b>	This command can be executed only if the profile is deactivated.
<b>Example</b>	<code>SEFOS (config-profile)# permit</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ip igmp snooping multicast-vlan profile</code> – Configures profile ID-to-VLAN mapping for multicast VLAN classification.</li><li>• <code>ip mcast profile</code> – Creates or modifies a multicast profile.</li><li>• <code>no profile active</code> – Deactivates the profile entry.</li><li>• <code>show ip mcast profile</code> – Displays the filters configured in the profile and the profile statistics.</li></ul>

---

## 41.5 deny

---

<b>Command Objective</b>	This command configures the action for the profile as deny. When the profile action is deny, the matching rule is not found in the table. The client report is not processed.
<b>Syntax</b>	<code>deny</code>
<b>Mode</b>	Profile Configuration Mode
<b>Package</b>	Workgroup and Metro_E
<b>Default</b>	The profile action is deny.
<u>Note:</u>	This command can be executed only if the profile is deactivated.
<b>Example</b>	<code>SEFOS (config-profile)# deny</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ip mcast profile</code> – Creates or modifies a multicast profile.</li><li>• <code>no profile active</code> – Deactivates the profile entry.</li><li>• <code>show ip mcast profile</code> – Displays the filters configured in the profile and the profile statistics.</li></ul>

---

## 41.6 range

---

**Command Objective** This command creates or modifies a filter. The filter entry is created based on the range of address provided by the administrator. If address is not configured, it is considered as a wild card (that is, the address is configured as 0.0.0.0).

The no form of this command deletes a filter.

---

**Syntax**

```
range <group-start-addr> [<group-end-addr>] [source
<source-start-addr> [<source-end-addr>]] [filter-mode
{include | exclude}]

no range <group-start-addr> [<group-end-addr>] [source
<source-start-addr> [<source-end-addr>]]
```

---

**Parameter Description**

- **<group-start-addr>** – Configures the multicast group address, which would be the start of multicast group address range.
- **<group-end-addr>** – Configures the multicast group address, which would be the end of multicast group address range.
- **<source-start-addr>** – Configures the multicast source address, which would be the start of multicast source address range.
- **<source-end-addr>** – Configures the multicast source address, which would be the end of multicast source address range.
- **filter-mode** – Configures the type of packets to be filtered.
  - **include** – Applies filter to include IGMP/MLD reports.
  - **exclude** – Applies filter to exclude IGMP/MLD reports.

---

**Mode** Profile Configuration Mode

---

**Package** Workgroup and Metro\_E

---

**Default** Any

---

**Note:** This command can be executed only if the profile is deactivated.

---

**Example** SEFOS(config-profile)# range 225.0.0.1 227.0.0.1 source 34.0.0.1 38.0.0.1 filter-mode include

---

**Related Command(s)**

- **ip mcast profile** – Creates or modifies a multicast profile.
  - **no profile active** – Deactivates the profile entry.
  - **show ip mcast profile** – Displays the filters configured in the profile.
-



## 41.7 profile active

---

<b>Command Objective</b>	This command activates the profile entry. When active, the profile is matched with the client report.  The no form of this command deactivates the profile entry.
<b>Syntax</b>	<code>profile active</code>  <code>no profile active</code>
<b>Mode</b>	Profile Configuration Mode
<b>Package</b>	Workgroup and Metro_E
<b>Example</b>	<code>SEFOS (config-profile)# profile active</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <code>ip igmp snooping multicast-vlan profile</code> – Configures profile ID-to-VLAN mapping for multicast VLAN classification.</li><li>• <code>ip igmp snooping ratelimit</code> – Configures the rate limit for a downstream interface in units of the number of IGMP packets per second.</li><li>• <code>ip igmp snooping limit</code> – Configures the maximum limit type for an interface.</li><li>• <code>ip igmp snooping filter-profileId</code> – Configures the multicast profile index for a downstream interface.</li><li>• <code>permit</code> – Configures the action for the profile as permit.</li><li>• <code>deny</code> – Configures the action for the profile as deny.</li><li>• <code>range</code> – Creates or modifies a filter.</li><li>• <code>ip mcast profile</code> – Creates or modifies a multicast profile.</li></ul>

---

## 41.8 show ip mcast profile

---

<b>Command Objective</b>	This command displays the filters configured in the profile and the profile statistics.
<b>Syntax</b>	<b>show ip mcast profile [&lt;profile-id&gt;] [statistics]</b>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>&lt;profile-id&gt;</b> - Displays the profile identifier for the multicast profile entry.</li><li>• <b>statistics</b> - Displays the statistics about the particular profile.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup and Metro_E
<b>Example</b>	<pre>SEFOS# show ip mcast profile Profile 1 sample   permit   range 225.0.0.1 227.0.0.1 source 34.0.0.1 38.0.0.1 mode include   range 227.0.0.1 227.0.0.1   range 228.0.0.1 230.0.0.1 mode exclude Profile 2   range 225.0.0.1 227.0.0.1 mode include   range 227.0.0.1 227.0.0.1   range 228.0.0.1 230.0.0.1 source 40.0.0.1 45.0.0.1 mode exclude  SEFOS# show ip mcast profile statistics Profile 1 sample   Port Reference count 1   Vlan Reference count 1 Profile 2   Port Reference count 0   Vlan Reference count 0</pre>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>ip mcast profile / ip igmp profile</b> – Creates or modifies a multicast profile.</li><li>• <b>permit</b> – Configures the action for the profile as permit.</li></ul>

---

- 
- **deny** – Configures the action for the profile as deny.
  - **range** – Creates or modifies a filter.
  - **ip igmp snooping multicast-vlan profile** – Configures profile ID-to-VLAN mapping for multicast VLAN classification.
  - **ip igmp snooping filter-profileId** – Configures the multicast profile index for a downstream interface.
-

## 41.9 debug tacm

---

**Command Objective** This command enables the generation of trace messages in TAC module. Trace messages are generated when there is an error, event, or occurrence of a specified action in the module.

The no form of this command disables the generation of trace messages.

---

**Syntax**

```
debug tacm {all | [entry] [exit] [filter] [critical]
[init-shut] [mgmt] [ctrl] [resource] [all-fail]}

no debug tacm {all | [entry] [exit] [filter] [critical]
[init-shut] [mgmt] [ctrl] [resource] [all-fail]}
```

---

**Parameter Description**

- **All** - Generates trace messages for all types of traces.
- **Entry** - Generates trace messages for all functions entered in the module.
- **Exit** - Generates trace messages for all the functions exited.
- **filter** - Generates trace messages for filter-related events.
- **critical** - Generates traces messages for critical errors which need immediate attention.
- **init-shut** - Generates trace messages for initialization and shutdown.
- **mgmt** - Generates debug statements for management plane functionality traces.
- **ctrl** - Generates debug statements for control plane functionality traces.
- **resource** - Generates debug statements for traces with respect to allocation and freeing of all resources except the buffers.
- **all-fail** - Generates trace messages for all types of failures.

---

**Mode** Privileged EXEC Mode

---

**Package** Workgroup and Metro\_E

---

**Example** SEFOS# debug tacm critical

---

## **CHAPTER 42**

# **RMON**

---

RMON (Remote Monitoring) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data.

The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. As such, RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.

## 42.1 set rmon

---

<b>Command Objective</b>	This command is used to enable or disable the RMON feature.
<b>Syntax</b>	<code>set rmon {enable   disable}</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>enable</b> - Enables the RMON feature in the system. On enabling, the RMON starts monitoring the networks, both local and remote, and provides network fault diagnosis.</li><li>• <b>disable</b> - Disables the RMON feature in the system. On disabling, the RMON's network monitoring is called off.</li></ul>
<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	Disabled
<b>Example</b>	<code>SEFOS(config)# set rmon enable</code>
<b>Related Command(s)</b>	<ul style="list-style-type: none"><li>• <b>show rmon</b> - Displays the RMON statistics, alarms, events, and history configured on the interface.</li></ul>

---

## 42.2 rmon collection history

---

**Command Objective** This command enables history collection of interface or VLAN statistics in the buckets for the specified time interval.

The no form of the command disables the history collection on the interface or VLAN.

---

**Syntax** `rmon collection history <index (1-65535)> [buckets <bucket-number (1-65535)>] [interval <seconds (1-3600)>] [owner <ownername (127)>]`

`no rmon collection history <index (1-65535)>`

---

**Parameter Description**

- `<index (1-65535)>` - Identifies an entry in the history control table. Each such entry defines a set of samples at a particular interval for an interface on the device. This value ranges from 1 to 65535.
- `buckets<bucket-number (1-65535)>` - Configures the number of buckets desired for the RMON collection history group of statistics. This is the requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this History Control Entry. The polling cycle is the bucket interval where the interface statistics details are stored. This value ranges from 1 to 65535.
- `interval<seconds (1-3600)>` - Configures the time interval over which the data is sampled for each bucket. This value ranges from 1 to 3600.
- `owner<ownername (127)>` - Configures the name of the owner of the RMON group of statistics.

---

**Mode** Interface Configuration Mode / Config VLAN Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Default**

- bucket number - 50
- interval - 1800 seconds

---

Note: In Config VLAN mode, this command executes only if either VLAN is set as active or if the member ports are associated with the VLAN.

---

**Example** **Interface Configuration Mode**

```
SEFOS(config) interface extreme-ethernet 0/1
```

```
SEFOS(config-if)# rmon collection history 1 buckets 2
```

---

---

```
interval 20
```

### Config VLAN Mode

```
SEFOS(config) vlan 1
```

```
SEFOS(config-vlan) rmon collection history 2
```

---

### Related Command(s)

- `vlan active` - Activates a VLAN in the switch.
  - `ports`- Configures a VLAN entry with the required member ports, untagged ports, or forbidden ports, and activates the VLAN.
  - `show rmon` - Displays the history collection for the configured bucket.
-



## 42.3 rmon collection stats

---

**Command Objective** This command enables RMON statistics collection on the interface or VLAN.

The no form of the command disables RMON statistics collection on the interface or VLAN.

---

**Syntax** `rmon collection stats <index (1-65535)> [owner <ownername (127)>]`

`no rmon collection stats <index (1-65535)>`

---

**Parameter Description**

- `<index (1-65535)>` - Identifies an entry in the statistics table. This value ranges from 1 to 65535.
- `owner <ownername (127)>` - Configures the name of the owner of the RMON group of statistics.

---

**Mode** Interface Configuration Mode / Config VLAN Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

Note: In Config VLAN mode, this command executes only if either VLAN is set as active or if the member ports are associated with the VLAN.

---

**Example**

**Interface Configuration Mode**

```
SEFOS(config) interface extreme-ethernet 0/1
SEFOS(config-if)# rmon collection stats 1
```

**Config VLAN Mode**

```
SEFOS(config) vlan 1
SEFOS(config-vlan) rmon collection stats 2
```

---

**Related Command(s)**

- `vlan active` - Activates a VLAN in the switch.
- `ports` - Configures a VLAN entry with the required member ports, untagged ports, or forbidden ports, and activates the VLAN.
- `show rmon` - Displays the RMON collection statistics.

---

## 42.4 rmon event

---

**Command Objective** This command adds an event to the RMON event table. The added event is associated with an RMON event number.

The no form of the command deletes an event from the RMON event table.

---

**Syntax**

```
rmon event <number (1-65535)> [description <event-  
description (127)>] [log] [owner <ownername (127)>] [trap  
<community (127)>]
```

```
no rmon event <number (1-65535)>
```

---

**Parameter Description**

- **<number (1-65535)>** - Sets the number of events to be added in the event table. This value ranges from 1 to 65535.
- **description<event-description (127)>** - Provides a description for the event. This value is a string with a maximum length of 127.
- **log** - Creates an entry in the log table for each event.
- **owner<ownername (127)>** - Displays the entity that are configured on this entry. This value is a string with a maximum value of 127.
- **trap<community (127)>** - Generates a trap. The SNMP community string is to be passed for the specified trap. This value is a string with a maximum value of 127.

---

**Mode** Global Configuration Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Example** SEFOS(config)# rmon event 1 log owner oracle trap netman

---

**Related Command(s)**

- **rmon alarm** - Sets an alarm on a MIB object.
- **show rmon** - Displays the RMON events (show rmon events).
- **show snmp community** - Configures the SNMP community details.

---

## 42.5 rmon alarm

---

**Command Objective** This command sets an alarm on a MIB object. The Alarm group periodically takes statistical samples from variables in the probe and compares them to thresholds that have been configured.

The no form of the command deletes the alarm configured on the MIB object.

---

**Syntax**

```
rmon alarm <alarm-number> <mib-object-id (255)> <sample-  
interval-time (1-65535)> {absolute | delta} rising-  
threshold <value (0-2147483647)> [rising-event-number (1-  
65535)] falling-threshold <value (0-2147483647)> [falling-  
event-number (1-65535)] [owner <ownername (127)>]
```

```
no rmon alarm <number (1-65535)>
```

---

**Parameter Description**

- **<alarm-number>/ <number (1-65535)>** - Displays the value of the statistic during the last sampling period. This value remains available until the current sampling period is completed. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This value is compared with the rising and falling thresholds. This value ranges from 1 to 65535.
  - **<mib-object-id (255)>** - Identifies the MIB object.
  - **<sample-interval-time (1-65535)>** - Identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular level for a MIB object in the device. This value ranges from 1 to 65535 seconds.
  - **absolute** - Compares the value of the selected variable with the thresholds at the end of the sampling interval.
  - **delta** - Subtracts the value of the selected variable at the last sample from the current value. The difference is compared with the thresholds at the end of the sampling interval.
  - **rising-threshold <value (0-2147483647)>** - Configures the rising threshold value. If the startup alarm is set as Rising alarm or RisingOrFalling alarm and if the configured threshold value is reached, then an alarm is raised. When the current sampled value is greater than or equal to the configured Rising threshold, and the value at the last sampling interval is less than this configured threshold, a single event will be generated. This value ranges from 0 to 2147483647.
  - **<rising-event-number (1-65535)>** - Raises the index of the event when the Rising threshold is reached. The event entry, identified by a particular value of this index, is the same as identified by the same value of
-

---

the event index object. This value ranges from 1 to 65535.

- **falling-threshold <value (0-2147483647)>** - Configures the falling threshold value. If the startup alarm is set as Falling alarm or RisingOrFalling alarm and if the configured threshold value is reached, then an alarm is raised. When the current sampled value is lesser than or equal to the configured Falling threshold, and the value at the last sampling interval is greater than this threshold, a single event will be generated. This value ranges from 0 to 2147483647.
- **<falling-event-number (1-65535)>** - Raises the index of the event when the Falling threshold is reached. The event entry, identified by a particular value of this index, is the same as identified by the same value of the event index object. This value ranges from 1 to 65535.
- **owner<ownername (127)>** - Sets the entity that are configured on this entry.

---

<b>Mode</b>	Global Configuration Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Default</b>	By default, the least event number in the event table is assigned for the rising and falling threshold as its event number.

---

Note:

- RMON events must have been configured.
- RMON collection stats must be configured.
- In Oracle SEFOS, we cannot monitor all the MIB objects through RMON. This will be applicable only to the Ethernet interfaces and VLANs.

---

<b>Example</b>	<pre>SEFOS(config)# rmon alarm 1 1.3.6.1.2.1.16.1.1.1.5.2 1 delta rising-threshold 2 falling-threshold 1</pre>
----------------	--

---

- |                           |   |
|---------------------------|---|
| <b>Related Command(s)</b> | <ul style="list-style-type: none"><li>• <b>rmon collection stats</b> - Enables RMON statistics collection on the interface.</li><li>• <b>rmon event</b> - Adds an event to the RMON event table.</li><li>• <b>show rmon</b> - Displays the RMON alarms (<code>show rmon alarms</code>).</li></ul> |
|---------------------------|---|
-

## 42.6 show rmon

---

<b>Command Objective</b>	This command displays the RMON statistics, alarms, events, and history configured on the interface.
<b>Syntax</b>	<code>show rmon [statistics [&lt;stats-index (1-65535)&gt;]] [alarms] [events] [history [history-index (1-65535)] [overview]]</code>
<b>Parameter Description</b>	<ul style="list-style-type: none"><li>• <b>statistics</b> - Displays a collection of statistics for a particular Ethernet interface. The probe for each monitored interface on this device measures the statistics.</li><li>• <b>alarms</b> - Displays the value of the statistics during the last sampling period. This value remains available until the current sampling period is completed.</li><li>• <b>events</b> - Generates events whenever an associated condition takes place in the device. The conditions may be alarms. Alarms are generated when a sampled statistical variable value exceeds the defined threshold value. The alarm module calls the events module.</li><li>• <b>history</b> - Displays the history of the configured RMON.</li><li>• <b>overview</b> - Displays only the overview of RMON history entries.</li></ul>
<b>Mode</b>	Privileged EXEC Mode
<b>Package</b>	Workgroup, Enterprise, Metro_E, and Metro
<b>Example</b>	<pre>SEFOS# show rmon statistics RMON is enabled Collection 4 on Vlan 1 is active, and owned by monitor, Monitors Vlan 1 which has Received 0 octets, 0 packets, 0 broadcast and 0 multicast packets, 0 undersized and 0 oversized packets, 0 fragments and 0 jabbers, 0 CRC alignment errors and 0 collisions. 0 out FCS errors, # of packets received of length (in octets): 64: 0, 65-127: 0, 128-255: 0, 256-511: 0, 512-1023: 0, 1024-1518: 0 Collection 45 on Ex0/1 is active, and owned by monitor,</pre>

---

---

```

Monitors ifEntry.1.1 which has
Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
0 out FCS errors,
# of packets received of length (in octets):
64: 0, 65-127: 0, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518: 0
Collection 56 on Vlan 5 is active, and owned by monitor,
Monitors Vlan 5 which has
Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
0 out FCS errors,
# of packets received of length (in octets):
64: 0, 65-127: 0, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518: 0
Number of statistics collection on interface: 1
Number of statistics collection on Vlan      : 2

SEFOS# show rmon
RMON is enabled

SEFOS# show rmon history
RMON is disabled
Entry 1 is active, and owned by monitor
Monitors ifEntry.1.2 every 1800 second(s)
Requested # of time intervals, ie buckets, is 50,
Granted # of time intervals, ie buckets, is 50,
Entry 4 is active, and owned by monitor
Monitors Vlan 40 every 1800 second(s)
Requested # of time intervals, ie buckets, is 50,
Granted # of time intervals, ie buckets, is 50,
Number of history collection on interface: 1

```

---

---

Number of history collection on Vlan : 1

**SEFOS# show rmon events**

RMON is enabled

Event 1 is active, owned by

Description is

Event firing causes nothing,

Time last sent is Aug 27 18:30:01 2009

Event 2 is active, owned by

Description is

Event firing causes nothing,

Time last sent is Aug 27 18:31:36 2009

**SEFOS# show rmon alarms**

RMON is enabled

Alarm 1 is active, owned by

Monitors 1.3.6.1.2.1.16.1.1.1.5.2 every 1 second(s)

Taking delta samples, last value was 0

Rising threshold is 2, assigned to event 1

Falling threshold is 1, assigned to event 1

On startup enable rising or falling alarm

**SEFOS# show rmon statistics 2 alarms events history 1**

RMON is enabled

Collection 2 on Ex0/1 is active, and owned by monitor,

Monitors ifEntry.1.1 which has

Received 5194 octets, 53 packets,

0 broadcast and 0 multicast packets,

0 undersized and 0 oversized packets,

0 fragments and 0 jabbers,

53 CRC alignment errors and 0 collisions.

# of packets received of length (in octets):

64: 0, 65-127: 53, 128-255: 0,

256-511: 0, 512-1023: 0, 1024-1518: 0

Alarm 4 is active, owned by Oracle

Monitors 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 every  
2 second(s)

Taking absolute samples, last value was 3

Rising threshold is 2, assigned to event 2

---

---

Falling threshold is 1, assigned to event 2  
On startup enable rising or falling alarm

Event 1 is active, owned by  
Description is  
Event firing causes nothing,  
Time last sent is Aug 27 18:30:01 2009

Event 2 is active, owned by  
Description is  
Event firing causes nothing,  
Time last sent is Aug 27 18:31:36 2009

**SEFOS# show rmon history overview**

RMON is enabled  
Entry 1 is active, and owned by monitor  
Monitors ifEntry.1.2 every 1800 second(s)  
Requested # of time intervals, ie buckets, is 50,  
Granted # of time intervals, ie buckets, is 50,  
Entry 4 is active, and owned by monitor  
Monitors Vlan 40 every 1800 second(s)  
Requested # of time intervals, ie buckets, is 50,  
Granted # of time intervals, ie buckets, is 50,  
Number of history collection on interface: 1  
Number of history collection on Vlan : 1

---

**Related Command(s)**

- **set rmon** - Enables or disables the RMON feature.
  - **rmon collection history** - Enables history collection of interface or VLAN statistics in the buckets for the specified time interval.
  - **rmon collection stats** - Enables RMON statistics collection on the interface or VLAN.
  - **rmon event** - Adds an event to the RMON event table.
  - **rmon alarm** - Sets an alarm on a MIB object.
-



## **CHAPTER 43**

# **RMON2**

---

RMONv2 is an extension of the RMON that deals with the information at the physical and data link network levels to support monitoring and protocol analysis of LANs. RMONv2 adds support for network and application layer monitoring.

RMONv2 is a portable implementation of Remote Network Monitoring version 2. RMONv2 is implemented with nine RMON MIB groups. They are Protocol directory, Protocol distribution, Address Map, Network Layer Host, Network Layer Matrix, Application Layer Host, Application layer Matrix, User History collection, and Probe configuration groups. RMONv2 provides extensions to four RMONv1 tables. They are etherStats table, historyControl table, hostControl table, and matrixControl table. RMON should be enabled for configuring the RMONv1 tables.

## 43.1 rmon2

---

**Command Objective** This command enables or disables RMON2 module in the switch. RMON2 lists the inventory of protocols, lists MAC address to network address bindings, tracks the amount of traffic between network addresses, and so on. The default value is disabled.

---

**Syntax** `rmon2 {enable | disable}`

---

**Parameter Description**

- **enable** - Enables the RMON2 module in the switch. Resources are allocated to the module.
- **disable** - Disables the RMON2 module in the switch. Resources allocated are released back to the system.

---

**Mode** Global Configuration Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Default** disabled

---

**Example** `SEFOS(config)# rmon2 enable`

---

## 43.2 debug rmon2

---

**Command Objective** This command configures various RMON2 debug trace messages.

The no form of the command disables the debug feature for RMON2 module. Debug facility captures events, errors, and the level of severity of the traces and logs them in a file.

---

**Syntax**

```
debug rmon2 {[func-entry][func-exit][critical][mem-  
fail][debug] | [ALL]}
```

```
no debug rmon2
```

---

**Parameter Description**

- **func-entry** - Generates Function Entry Trace messages. When a function is called in the RMON2 module, the details of the function are displayed in the trace message. The traces are captured for all the functions in RMON2.
- **func-exit** - Generates Function Exit Trace messages. When the system completes a function and exits, the details of the function exited are displayed in the trace messages. The traces are captured for all functions.
- **critical** - Generates Critical Trace messages. The errors that cause damage or malfunctioning of the system are displayed as critical traces.
- **mem-fail** - Generates Memory Failure Trace messages. When there is a constraint for memory allocation when a function is initiated, the mem-fail trace is displayed.
- **debug** - Generates Debug Trace messages for less severe errors and events.
- **ALL** - Generates all kinds of trace messages mentioned above.

---

**Mode** Privileged EXEC Mode

---

**Package** Workgroup, Enterprise, Metro\_E, and Metro

---

**Example** SEFOS# debug rmon2 ALL

---